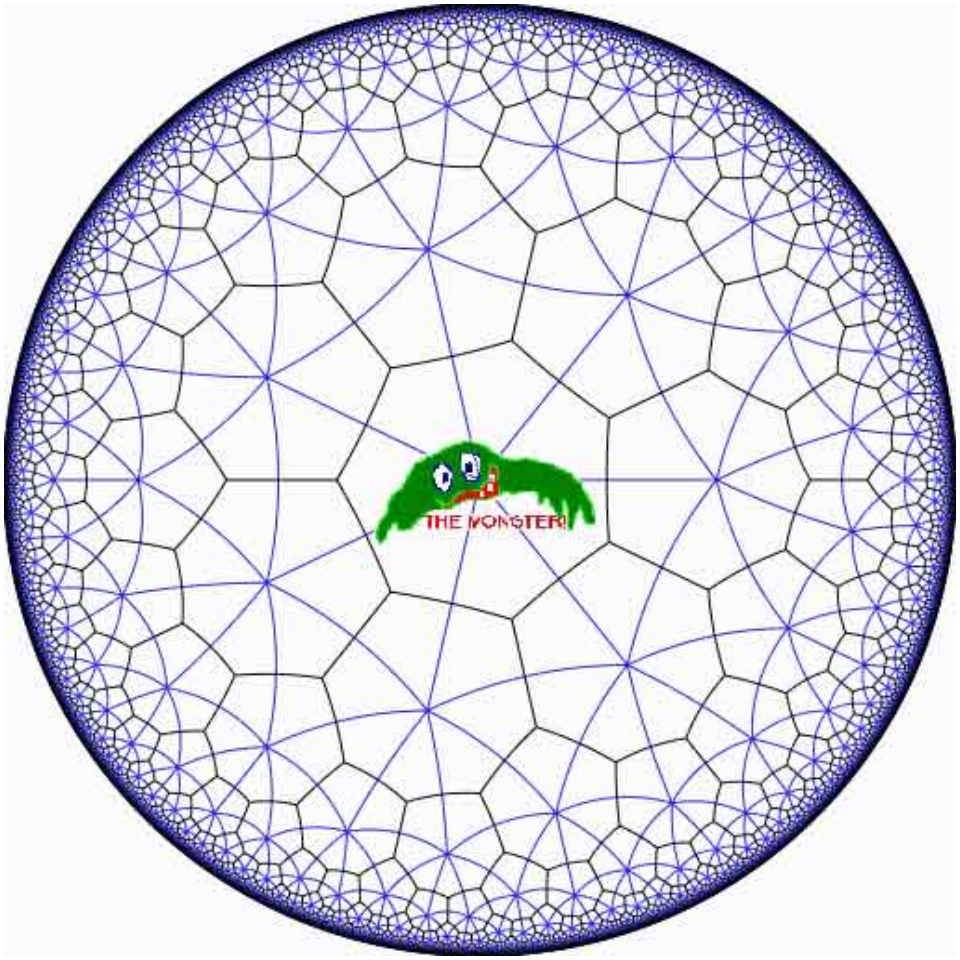
Monsters and Moonshine

lieven le bruyn



2012

universiteit antwerpen
neverendingbooks.org

CONTENTS

series 1

MONSTERS

1.1 The Scottish solids

John McKay pointed me to a few interesting links on 'Platonic' solids and monstrous moonshine. If you thought that the ancient Greek discovered the five Platonic solids, think again!

They may have been the first to give a correct proof of the classification but the regular solids were already known in 2000BC as some neolithic stone artifacts discovered in Scotland show.

These Scottish solids can be visited at the Ashmolean Museum in Oxford. McKay also points to the paper Polyhedra in physics, chemistry and geometry by Michael Atiyah and Paul Sutcliffe.

He also found my posts on a talk I gave on monstrous moonshine for 2nd year students earlier this year and mentionted a few errors and updates. As these posts are on my old weblog I'll repost and update them here soon.

For now you can already hear and see a talk given by John McKay himself 196884=1+196883, a monstrous tale at the Fields Institute.

1.2 The Scottish solids hoax

A truly good math-story gets spread rather than scrutinized. And a good story it was : more than a milenium before Plato, the Neolithic Scottish Math Society classified the five regular solids : tetrahedron, cube, octahedron, dodecahedron and icosahedron. And, we had solid evidence to support this claim : the NSMS mass-produced stone replicas of their finds and about 400 of them were excavated, most of them in Aberdeenshire.

Six years ago, Michael Atiyah and Paul Sutcliffe arXived their paper Polyhedra in physics, chemistry and geometry, in which they wrote :

"Although they are termed Platonic solids there is convincing evidence that they were known to the Neolithic people of Scotland at least a thousand years before Plato, as demon-

strated by the stone models pictured in g. 1 which date from this period and are kept in the Ashmolean Museum in Oxford. ”

Fig. 1 is the picture below, which has been copied in numerous blog-posts (including my own, see the previous section) and virtually every talk on regular polyhedra.

From left to right, stone-ball models of the cube, tetrahedron, dodecahedron, icosahedron and octahedron, in which ’knobs’ correspond to ’faces’ of the regular polyhedron, as best seen in the central dodecahedral ball.

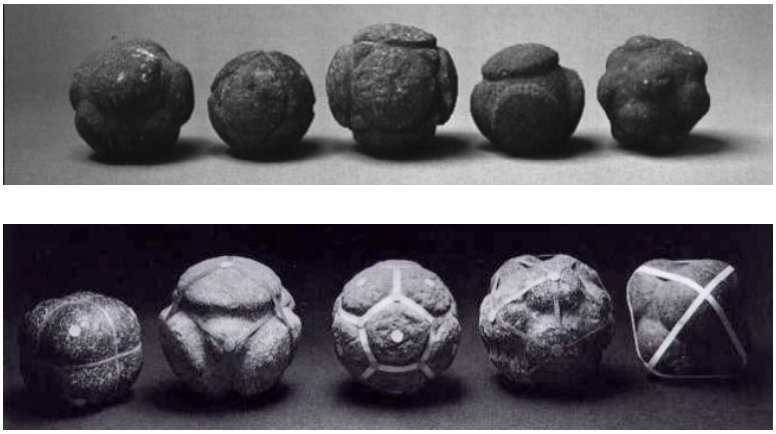
But then ... where’s the icosahedron? The fourth ball sure looks like one but only because someone added ribbons, connecting the centers of the different knobs. If this ribbon-figure is an icosahedron, the ball itself should be another dodecahedron and the ribbons illustrate the fact that icosa- and dodeca-hedron are dual polyhedra. Similarly for the last ball, if the ribbon-figure is an octahedron, the ball itself should be another cube, having exactly 6 knobs. Who did adorn these artifacts with ribbons, thereby multiplying the number of ’found’ regular solids by two (the tetrahedron is self-dual)?

The picture appears on page 98 of the book Sacred Geometry (first published in 1979) by Robert Lawlor. He attributes the NSMS-idea to the book Time Stands Still: New Light on Megalithic Science (also published in 1979) by Keith Critchlow. Lawlor writes

”The five regular polyhedra or Platonic solids were known and worked with well before Plato’s time. Keith Critchlow in his book Time Stands Still presents convincing evidence that they were known to the Neolithic peoples of Britain at least 1000 years before Plato. This is founded on the existence of a number of sphericalfstones kept in the Ashmolean Museum at Oxford. Of a size one can carry in the hand, these stones were carved into the precise geometric spherical versions of the cube, tetrahedron, octahedron, icosahedron and dodecahedron, as well as some additional compound and semi-regular solids, such as the cube-octahedron and the icosidodecahedron.”

Critchlow says, ’What we have are objects clearly indicative of a degree of mathematical ability so far denied to Neolithic man by any archaeologist or mathematical historian’. He speculates on the possible relationship of these objects to the building of the great astronomical stone circles of the same epoch in Britain: ’The study of the heavens is, after all, a spherical activity, needing an understanding of spherical coordinates. If the Neolithic inhabitants of Scotland had constructed Maes Howe before the pyramids were built by the ancient Egyptians, why could they not be studying the laws of three-dimensional coordinates? Is it not more than a coincidence that Plato as well as Ptolemy, Kepler and Al-Kindi attributed cosmic significance to these figures?’ ”

As Lawlor and Critchlow lean towards mysticism, their claims should not be taken for granted. So, let’s have a look at these famous stones kept in the Ashmolean Museum. The Ashmolean has a page dedicated to their Stone Balls, including the following picture (the Critchlow/Lawlor picture below, for comparison)



The Ashmolean stone balls are from left to right the artifacts with catalogue numbers :

- Stone ball with 7 knobs from Marnoch, Banff (AN1927.2728)
- Stone ball with 6 knobs and isosceles triangles between, from Fyvie, Aberdeenshire (AN1927.2731)
- Stone ball with 6 knobs and isosceles triangles between, from near Aberdeen (AN1927.2730)
- Stone ball with 4 knobs from Auchterless, Aberdeenshire (AN1927.2729)
- Stone ball with 14 knobs from Aberdeen (AN1927.2727)

Ashmolean's AN 1927.2729 may very well be the tetrahedron and AN 1927.2727 may be used to forge the 'icosahedron' (though it has 14 rather than 12 knobs), but the other stones sure look different. In particular, none of the Ashmolean stones has exactly 12 knobs in order to be a dodecahedron.

Perhaps the Ashmolean has a larger collection of Scottish balls and today's selection is different from the one in 1979? Well, if you have the patience to check all 9 pages of the Scottish Ball Catalogue by Dorothy Marshall (the reference-text when it comes to these balls) you will see that the Ashmolean has exactly those 5 balls and no others!

The sad lesson to be learned is : whether the Critchlow/Lawlor balls are falsifications or fabrications, they most certainly are NOT the Ashmolean stone balls as they claim!

Clearly this does not mean that no neolithic scott could have discovered some regular polyhedra by accident. They made an enormous amount of these stone balls, with knobs ranging from 3 up to no less than 135! All I claim is that this ball-carving thing was more an artistic endeavor, rather than a mathematical one.

There are a number of musea having a much larger collection of these stone balls. The Hunterian Museum has a collection of 29 and some nice online pages on them, including 3D animation. But then again, none of their balls can be a dodecahedron or icosahedron (according to the stone-ball-catalogue).

In fact, more than half of the 400+ preserved artifacts have 6 knobs. The catalogue tells that there are only 8 possible candidates for a Scottish dodecahedron (below their catalogue numbers, indicating for the knowledgeable which museum owns them and where they were found)

- NMA AS 103 : Aberdeenshire

- AS 109 : Aberdeenshire
- AS 116 : Aberdeenshire (prob)
- AUM 159/9 : Lambhill Farm, Fyvie, Aberdeenshire
- Dundee : Dyce, Aberdeenshire
- GAGM 55.96 : Aberdeenshire
- Montrose = Cast NMA AS 26 : Freelands, Glasterlaw, Angus
- Peterhead : Aberdeenshire

The case for a Scottish icosahedron looks even worse. Only two balls have exactly 20 knobs

- NMA AS 110 : Aberdeenshire
- GAGM 92 106.1. : Countesswells, Aberdeenshire

Here NMA stands for the National Museum of Antiquities of Scotland in Edinburg (today, it is called 'National Museums Scotland') and GAGM for the Glasgow Art Gallery and Museum. If you happen to be in either of these cities shortly, please have a look and let me know if one of them really is an icosahedron!

UPDATE:

Victoria White, Curator of Archaeology at the Kelvingrove Art Gallery and Museum, confirms that the Countesswells carved stone ball (1892.106.l) has indeed 20 knobs. She gave this additional information :

"The artefact came to Glasgow Museums in the late nineteenth century as part of the John Rae collection. John Rae was an avid collector of prehistoric antiquities from the Aberdeenshire area of Scotland. Unfortunately, the ball was not accompanied with any additional information regarding its archaeological context when it was donated to Glasgow Museums. The carved stone ball is currently on display in the 'Raiders of the Lost Art' exhibition."

Dr. Alison Sheridan, Head of Early Prehistory, Archaeology Department, National Museums Scotland makes the valid point that new balls have been discovered after the publication of the catalogue, but adds :

"Although several balls have turned up since Dorothy Marshall wrote her synthesis, none has 20 knobs, so you can rely on Dorothys list."

She has strong reservations against a mathematical interpretation of the balls :

"Please also note that the mathematical interpretation of these Late Neolithic objects fails to take into account their archaeological background, and fails to explain why so many do not have the requisite number of knobs! Its a classic case of people sticking on an interpretation in a state of ignorance. A great shame when so much is known about Late Neolithic archaeology."

1.3 Conway's M_{13} game

Recently, I've been playing with the idea of writing a book for the general public. The book's concept is simple : I would consider the mathematical puzzles creating an hype over the last three centuries : the 14-15 puzzle for the 19th century, Rubik's cube for the 20th century and, of course, Sudoku for the present century.

For each puzzle, I would describe its origin, the mathematics involved and how it can be used to solve the puzzle and, finally, what the differing quality of these puzzles tells us about mathematics' changing standing in society over the period. The final part of the book would then be more optimistic. What kind of puzzles should we promote for mathematical thinking to have a fighting chance to survive in the near future?

Fig. 1.1: John Conway

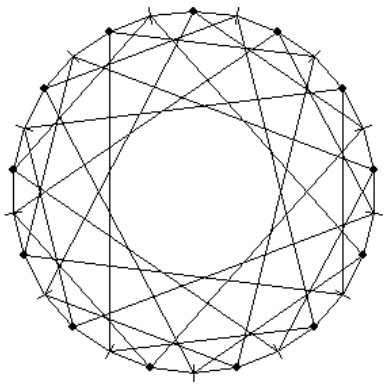
One of the puzzles I would propose is M_{13}, a sliding game first proposed by John Horton Conway in 1989 at the fourteenth New York Graph Theory Day. The analysis of the game was taken up by Jeremy Martin in his 1996 honors thesis in mathematics The Mathieu group M(12) and Conway's M(13)-game under the supervision of Noam Elkies.

Two years ago, the three of them joined forces and arXived the paper The Mathieu group M(12) and its pseudogroup extension M(13). The game is similar to the 15-puzzle replacing the role played by the simple alternating group A_{15} there with that of the sporadic simple Mathieu group M_{12}.

The game board of M_{13} is the finite projective plane $\mathbb{P}^2(\mathbb{F}_3)$ over the field with three elements $\mathbb{F}_3$. Recall that the number of points in projective n-space over a finite field of q-elements $\mathbb{P}^n(\mathbb{F}_q)$ is given by

$$q^n + q^{n-1} + \cdots + q + 1$$

Therefore, there are 13=9+3+1 points on the board and as there is a bijection between points and lines in the projective plane, there are also 13 lines on the board, each containing exactly 4=3+1 points and so each point lies on exactly 4 lines. Moreover, two distinct points p and q determine a unique line $\overline{pq}$ and two distinct lines l and m have a unique intersection point $l \cap m = p$.



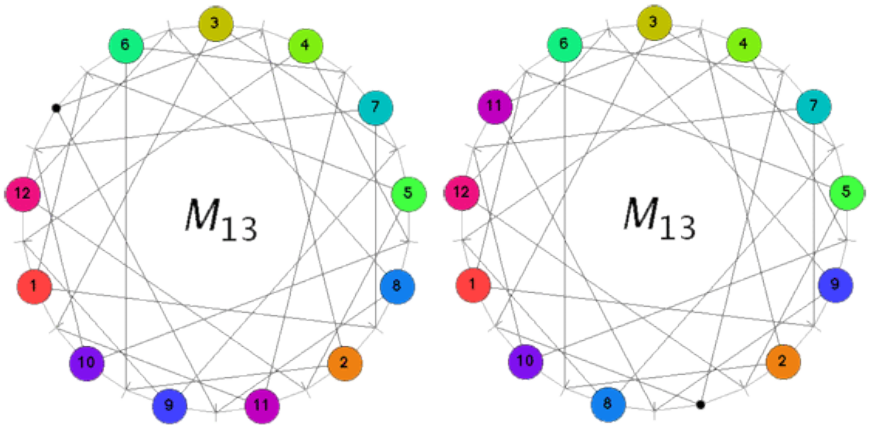
Clearly it will be hard selling a projective plane board to the general public, so let us depict all this information in a more amenable form such as the figure on the left.

The 13 points are indicated by the small discs around the circle whereas the 13 lines are depicted as small strokes on the circle. All edges (both 'along' as well 'inside' the circle) connect a point p and a line l subject to the relation that p lies on the line l in the projective plane $\mathbb{P}^2(\mathbb{F}_3)$.

The fact that two distinct points determine a unique line corresponds to the fact that for any two small-discs there is a unique small-stroke connecting both small-discs with an edge (note that one or both of these edges may lie on the circle). Similarly, for any two small-strokes the is a unique small-disc con-

nected via edges to the two small-strokes, corresponding to the fact that two lines have a unique point in common.

A typical position in Conway's puzzle M_{13} consists in placing numbered counters, labeled 1 through 12, on 12 of the 13 points leaving one point empty, called the "hole". A basic move consists of the following operation : choose a labeled point, say, p. Then, there is a unique line l (a small-stroke) containing p and the hole and there are two more points say q and r on this line l. The basic move replaces the counters between q and r and moves the counter of p to the hole and the hole to point p. For example, consider the position on the left



and suppose we want to move the counter 11 to the hole. Hole and 11 determine the unique line represented by the small-stroke immediately to the left of 11. This line contains the further points with counters 8 and 9. Hence, applying the basic move we get the situation on the right hand side. The aim of *Conway's game* M_{13} is to get the hole at the top point and all counters in order 1,2,...,12 when moving clockwise along the circle. One can play this puzzle online using the excellent java-applet by Sebastian Egner.

Another time we will make the connection with the Mathieu groupoid M_{13} and the sporadic simple Mathieu group M_{12}.

Reference : John H. Conway, Noam D. Elkies, and Jeremy L. Martin "The Mathieu group M(12) and its pseudogroup extension M(13)"

1.4 The 15-puzzle groupoid (1/2)

Before we go deeper into Conway's M(13) puzzle 1.3, let us consider a more commonly known sliding puzzle: the 15-puzzle.

A heated discussion went on a couple of years ago at sci-physics-research, starting with this message. Lubos Motl argued that group-theory is sufficient to analyze the problem and that there is no reason to resort to groupoids ('The human(oids) who like groupoids...' and other goodies, in pre-blog but vintage Motl-speak) whereas 'Jason' defended his viewpoint that a groupoid is the natural symmetry for this puzzle.

I'm mostly with Lubos on this. All relevant calculations are done in the symmetric group S_{16} and (easy) grouptheoretic results such as the distinction between even and odd permutations or the generation of the alternating groups really crack the puzzle. At the same time, if one wants to present this example in class, one has to be pretty careful to avoid confusion

between permutations encoding positions and those corresponding to slide-moves. In making such a careful analysis, one is bound to come up with a structure which isn't a group, but is precisely what some people prefer to call a groupoid (if not a 2-group...).

Fig. 1.2: Heinrich Brandt

Groupoids are no recent invention but date back to 1926 when Heinrich Brandt defined what we now know as the 'Brandt groupoid' in his study of *noncommutative number theory*. He was studying central simple algebras (the noncommutative counterpart of number fields) in which there usually is not a unique 'ring of integers' (in noncommutative parlance, a maximal order) and fractional ideals have a left- and a right- maximal order associated to it, leading naturally to left- and right- unit elements and the notion of a groupoid.

The algebraic notion of a groupoid is a set G with a partial multiplication and an everywhere defined inverse satisfying associativity $a*(b*c) = (a*b)*c$ whenever the terms are defined. Further, whenever $a*b$ is defined one has $a^{-1}*a*b = b$ and $a*b*b^{-1} = a$ and finally all $a^{-1}*a$ and $a*a^{-1}$ are defined (but may be different elements). The categorical definition of a groupoid is even simpler : it is a category in which every morphism is an isomorphism. Both notions are equivalent.

Recall that the 15-puzzle is a 4x4 slide-puzzle with initial configuration with the hole at the right bottom square (see left) and one can slide the hole one place at a time in vertical or horizontal direction. For example, if one slides the hole along the path 12-11-7-6-2 one ends up with the situation on the right

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

(initial position)

1		3	4
5	2	6	8
9	10	7	11
13	14	15	12

(position after 12-11-7-6-2)

The mathematical aim is to determine the allowed positions, that is those which can be reached from the initial position by making legal slide moves. The puzzle aim is to return to the initial position starting from an allowed position. We will determine the number of allowed positions and why they are the elements of a groupoid.

We don't want to draw arrays all the time so we need a way to encode a position. Giving the hole label 16 we can record a position by writing down the permutation on 16 letters describing by which label in the given position, the label of the initial position is replaced. For example, the situation on the right arises by leaving 1 to position 1, 2 is replaced by 16, 3,4 and 5 are left in their position but 6 is replaced by 2 and so on. So, we can encode this position by the permutation $\sigma = (2, 16, 12, 11, 7, 6)$ and conversely, given such a permutation we can fill in the entire position encoded by it. We will denote the array or position corresponding to a partition $\tau \in S_{16}$ by the boxed symbol $\boxed{\tau}$.

Next, we turn to slide-moves. A basic move interchanges the hole (label 16) with a square labeled i (if i is a horizontal or vertical neighbor of the hole in the position) so can be represented by the transposition $(16, i)$. We can iterate this procedure, a legal move from a position $\boxed{\tau}$ will be a succession of basic-moves written from right to left as is usual in composing permutations

$(16, i_k) \cdots (16, i_2)(16, i_1)$

where legality implies that at each step the label i_{m+1} must be a vertical or horizontal neighbor of the hole in the position reached from $\boxed{\tau}$ after applying the move $(16, i_m)(16, i_{m-1}) \cdots (16, i_2)(16, i_1)$. Hence, we'd better have a method to compute the position we obtain from a given position by applying a legal sequence of slide-moves. The rule is : multiply the slide-move-permutation with the position-permutation in the group S_{16} to get the code for the obtained position. In symbols

$$(16, i_k) \cdots (16, i_2)(16, i_1)\boxed{\tau} = \boxed{(16, i_k) \cdots (16, i_2)(16, i_1)\tau}$$

For example, the initial position corresponds to the identity permutation, that is, is $\boxed{()}$ and applying to it the legal seuence of slides moved along the path 12-11-7-6-2 as before we get the position with code

$$(16, 2)(16, 6)(16, 7)(16, 11)(16, 12)\boxed{()} = \boxed{(16, 2)(16, 6)(16, 7)(16, 11)(16, 12)} = \boxed{(16, 12, 11, 7, 6, 2)}$$

which is indeed the code of the position obtained above on the right. Right, the basic ingredient to have full understanding of this puzzle are hence the combination of an allowed position together with a legal move-sequence starting from it. Therefore, we will take as our elements all possible combinations $\sigma\boxed{\tau}$ with $\sigma, \tau \in S_{12}$ where τ is the code of a reachable position and $\sigma = (16, i_l) \cdots (16, i_1)$ is a legal move from that position.

On this set of elements we only have a partially defined composition rule, for we can only make sense of the composition of moves

$$\sigma_1\boxed{\tau_1} * \sigma_2\boxed{\tau_2} = \sigma_1\sigma_2\boxed{\tau_2}$$

provided τ_1 is the code of the position reached from $\boxed{\tau_2}$ after applying the move-sequence σ_2, that is, the multiplication above is defined if and only if

$\tau_1 = \sigma_2\tau_2$ in S_{16}

All conditions of the algebraic notion of a groupoid are satisfied. For example, every element has an inverse

$(\sigma\boxed{\tau})^{-1} = \sigma^{-1}\boxed{\omega}$ where $\omega = \sigma\tau$ in S_{16}

and it is easy to check that all conditions are indeed satisfied. In the categorical definition, the groupoid is the category having as the objects the reachable positions, and morphisms $\boxed{\tau_1} \to \boxed{\tau_2}$ are of the form $\sigma_1\boxed{\tau_1}$ such that $\sigma_1\tau_1 = \tau_2$ (hence, all morphisms are isomorphisms and there is just one morphism between two objects, namely corresponding to $\sigma_1 = \tau_2\tau_1^{-1} \in S_{16}$. For example, each object $\boxed{\tau}$ also has an identity morphism $()\boxed{\tau}$ and again all categorical requirements are met.

This groupoid we will call the the *15-puzzle groupoid* and in the next section we will determine that it has exactly $\frac{1}{2}16!$ objects.

1.5 The 15-puzzle groupoid (2/2)

In the last section we have seen that the legal positions of the classical 15-puzzle are the objects of a category in which every morphism is an isomorphism (a groupoid). Today, we will show that there are exactly 10461394944000 objects (legal positions) in this groupoid. The crucial fact is that positions with the hole in a fixed place can be identified with the elements of the alternating group A_{15}, a fact first proved by William Edward Story in 1879 in a note published in the American Journal of Mathematics.

Recall that the positions reachable from the initial position can be encoded as $\boxed{\tau}$ where τ is the permutation on 16 elements (the 15 numbered squares and 16 for the hole) such that $\tau(i)$ tells what number in the position lies on square i of the initial position. The set of all reachable positions are the objects of our category. A morphism $\boxed{\tau} \to \boxed{\sigma}$ is a legal sequence of slide-moves starting from position $\boxed{\tau}$ and ending at position $\boxed{\sigma}$. That is,

$$\boxed{\sigma} = (16, i_k)(16, i_{k-1}) \cdots (16, i_2)(16, i_1)\boxed{\tau}$$

where for every number m between 1 and k we have that the number i_{m+1} is an horizontal or vertical neighbor of the hole in position $\boxed{(16, i_m) \cdots (16, i_1)\tau}$. When we identify such a morphism with the corresponding element $(16, i_k) \cdots (16, i_2)(16, i_1) \in S_{16}$ we see that it must be the unique element $\sigma\tau^{-1}$ hence there is just one morphism between two objects and they are all invertible, so our category is indeed a groupoid. Can we say something about the length k of such a sequence of slide moves? Well, consider the OXO-drawing on our 4x4 square

O	X	O	X
X	O	X	O
O	X	O	X
X	O	X	O

One legal slide-move brings an O-hole to an X-hole and an X-hole to an O-hole, so if the holes in $\boxed{\sigma}$ and $\boxed{\tau}$ are of the same type (both O-holes or both X-holes) then the length k of a legal sequence must be even and therefore the permutation $\sigma\tau^{-1} = (16, i_k) \cdots (16, i_1)$ belongs to the simple alternating group A_{16}.

In particular, if we take $\tau = ()$ the original position we see that if a reachable position σ has the hole in the bottom right corner (and hence σ fixes 16 so is an element of S_{15}) then

$$\sigma \in A_{16} \cap S_{15} = A_{15}$$

and in particular, Loyd's 14-15 puzzle has no solution (as it corresponds to the transposition $\sigma = (14, 15) \notin A_{15}$. This argument first appeared in print in W.W. Johnson "Note on the "15" puzzle" Amer. J. Math. 2 (1879) 397-399. We can compose legal sequences leading to positions having their hole at the bottom right in the groupoid showing that such positions can be identified with a subgroup of A_{15}. Note that we do NOT claim that we can

multiply any two sequences of even length $(16, i_k) \cdots (16, i_1)$ with $(16, j_l) \cdots (16, j_1)$ (which would give us the whole of A_{16}) but only composable morphisms in the groupoid!

W.E. Story then went on to show that this subgroup is the full alternating group A_{15} which comes down to finding enough reachable positions, with the hole at the bottom right, to generate the group. We will sketch a more recent argument due to Aaron Archer (Math. Monthly 106 (1999) 793-799). He starts out with another encoding of reachable positions, disregarding the exact placement of the hole. He records the 15-numbers in order along a snakelike path disregarding the hole.

→	→	→	↓
↓	←	←	←
→	→	→	↓
←	←	←	←

so the position

1	2	3	4
5	6	7	8
	15	12	14
13	9	11	10

is encoded as $[1, 2, 3, 4, 8, 7, 6, 5, 15, 12, 14, 10, 11, 9, 13]$. The point being that we can slide the hole along the snakelike path to get a uniquely determined position having the same code but with the hole at another position. For example, sliding the hole along the path upwards to the third square of the upper row we get the position

1	2		3
6	7	8	4
5	15	12	14
13	9	11	10

having the same code.

This gives a natural one-to-one correspondence between reachable positions having their hole at spot i with those having the hole on spot j, so in order to determine the number of objects in our groupoid, it suffices to count the number of reachable positions with the hole at a specified spot. They are just all the codes and as they form a subgroup of A_{15} it is enough to calculate the permutations induced on a code by just one slide-move. If the slide move is along the snakelike path, it will not alter the code, so we only have to compute 9 remaining slide modes S(1,8), S(2,7), S(3,6), S(7,10), S(6,11), S(5,12), S(9,16), S(10,15) and S(11,14) where the numbers correspond to the order in which we encounter the square along the snakelike path. For example S(1,8) is the slide move changing the hole at position (1,1) to position (2,1). This move has the following effect on a position

	a_1	a_2	a_3
a_7	a_6	a_5	a_4
a_8	a_9	a_{10}	a_{11}
a_{15}	a_{14}	a_{13}	a_{12}

moving to

a_7	a_1	a_2	a_3
	a_6	a_5	a_4
a_8	a_9	a_{10}	a_{11}
a_{15}	a_{14}	a_{13}	a_{12}

whence it has the effect of changing the code

$[a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}]$ to the code

$[a_7, a_1, a_2, a_3, a_4, a_5, a_6, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}]$

and therefore it corresponds to the permutation $S(1, 8) = (1, 7, 6, 5, 4, 3, 2)$. Similarly, one calculates that the other slide moves determine the following permutations

$S(2, 7) = (2, 6, 5, 4, 3), S(3, 6) = (3, 5, 4), S(5, 12) = (5, 11, 10, 9, 8, 7, 6)$

$S(6, 11) = (6, 10, 9, 8, 7), S(7, 10) = (7, 9, 8), S(9, 16) = (9, 15, 14, 13, 12, 11, 10)$

$S(10, 15) = (10, 14, 13, 12, 11), S(11, 14) = (11, 13, 12)$

(Ive replaced the permutations in Archer's paper by their inverses because I want to have left actions rather than right ones). The only thing left to do is to fire up GAP and verify that these permutations do indeed generate the full alternating group A_{15}. Summarizing, there are precisely $\frac{1}{2}15!$ reachable positions having their hole in a specified place and as

there are 16 possible places for the hole, we get that the total number of reachable positions (or if you prefer, the number of objects in our groupoid) is equal to

$$16 \times \tfrac{1}{2}15! = \tfrac{1}{2}16! = 10461394944000$$

and the whole point of the careful group versus groupoid analysis is that one should not make the mistake in interpreting this number as the number of elements of the alternating group A_{16}. For those who don't like categories but prefer the algebraic notion of a groupoid, their groupoid has

$$(10461394944000)^2 = 109440784174348763136000000$$

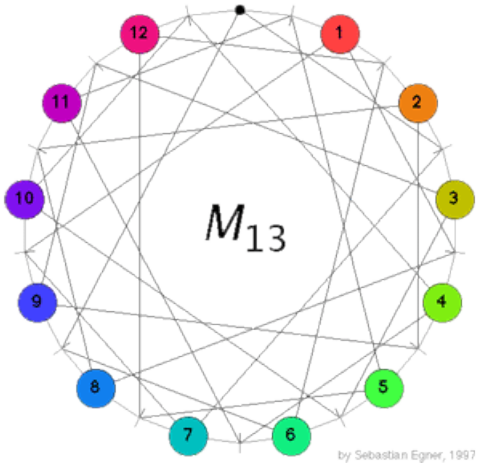
elements as there is exactly one morphism between two objects.

References :

1. Aaron F. Archer, "A Modern Treatment of the 15 Puzzle" Mathematical Monthly 106 (1999) 793-799

2. W.E. Story, "Note on the "15" puzzle", Amer. J. Math. 2 (1879) 399-404

1.6 Conway's M_{13}-groupoid (1/2)



Conway's puzzle M_{13} 1.3 is a variation on the 15-puzzle played with the 13 points in the projective plane $\mathbb{P}^2(\mathbb{F}_3)$. The desired position is given on the left where all the counters are placed at at the points having that label (the point corresponding to the hole in the drawing has label 0). A typical move consists in choosing a line in the plane going through the point where the hole is, choose one of the three remaining points on this line and interchange the counter on it for the hole while at the same time interchanging the counters on the other two points. In the drawing on the left, lines correspond to the little-strokes on the circle and edges describe which points lie on which lines. For example, if we want to move counter 5 to the hole we notice that both of them lie on the line represented by the stroke just to the right of the hole and this line contains also the two points with counters 1 and 11, so we have to replace these two counters too in making a move. Today we will describe the groupoid corresponding to this slide-puzzle so if you want to read on, it is best to play a bit with Sebastian Egner's M(13) Java Applet to see the puzzle in action (and to use it to verify the claims made below). Clicking on a counter performs the move taking the counter to the hole.

For the 15-puzzle I've gone to great lengths of detail in the last two sections explaining how a groupoid naturally crops up having as its objects the reachable positions and as its morphisms the legal slide-sequences. Here, I'll economize on details.

We can encode a position by a permutation in S_{13} by recording the counters (the hole having counter 0) as we move along the circle clockwise starting at the point of label 0 (the top-point). Basic moves transpose two pairs of counters so are given by a product

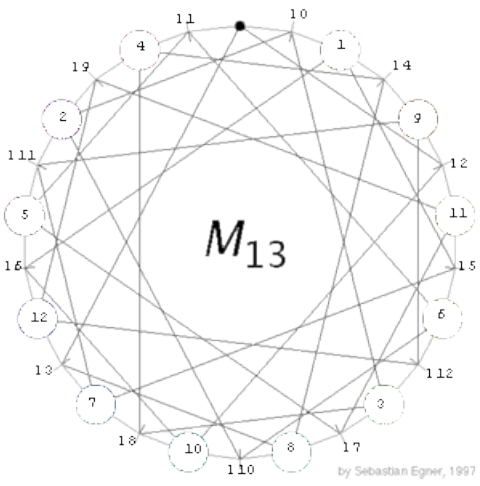
of two transpositions. For example, the move described above from the initial position is $(0,5)(1,11)$. Again it is clear how to make a groupoid from the reachable positions and the legal move-sequences and how all actual calculations can be done inside the group S_{13}. Two small remarks. (1) The situation is more symmetric than in the 15-puzzle. Here we have precisely 12 possible basic moves from any given position corresponding to the 12 non-hole counters which can be thrown into the hole. (2) Related to this, we have another way to encode move-sequences here. For each basic move we can jot down the *label* of the point whose counter we will throw to the hole (note : label, not counter!). The point of this being that we can now describe all reachable positions having the hole at the top point (the label 0 point) as those obtained from a move sequence of the form $[0-i_1-i_2-\ldots-i_k-0]$ for all choices of i_j between 0 and 12. However, not all these sequences give different positions and we want to determine how many distinct such positions we have. They will again form a subgroup of S_{12} and the aim will be to show that this subgroup is the sporadic simple Mathieu group M_{12}. We will check now that M_{12} is contained in this group. Next time we will prove the other inclusion.

Clearly, there are several different ways to label the 13 points and lines in the projective plane and unfortunately the choice of the Conway-Elkies-Martin paper is different from that of the Java Applet. For example, in the Applet-labeling 1,3,4,8 are on a line, whereas the paper-labeling assumes the following point/line labels

$l_0 = \{0,1,2,3\}, l_1 = \{0,4,5,6\}, l_2 = \{0,9,10,11\}, l_3 = \{0,7,8,12\}, l_4 = \{1,4,8,9\}$

$l_5 = \{1,6,7,11\}, l_6 = \{1,5,10,12\}, l_7 = \{3,5,8,11\}, l_8 = \{3,4,7,10\}$

$l_9 = \{2,4,11,12\}, l_{10} = \{2,6,8,10\}, l_{11} = \{2,5,7,9\}, l_{12} = \{3,6,9,12\}$



We need to find a dictionary between the two labeling-systems. Again there are several options, but here is the first one I found. Relabeling the points of the Applet as on the left (also indicated is the labeling of the lines) we get the labeling of the paper. Hence, to all CEM-paper-sequences we have to apply the *dictionary*

$0(0), 1(1), 2(11), 3(5), 4(12), 5(10), 6(4)$

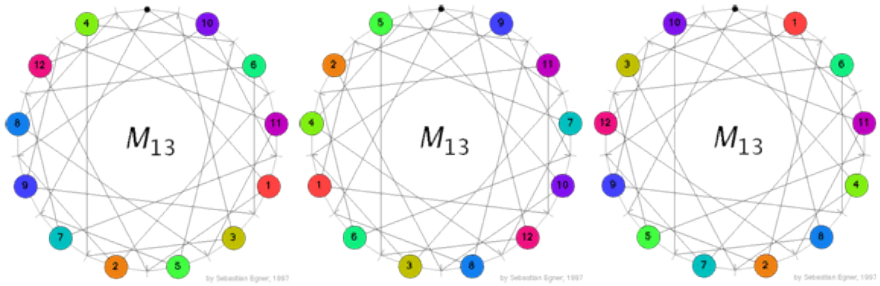
$7(8), 8(6), 9(2), 10(7), 11(3), 12(9)$

and use the bracketed labels to perform the sequence in the Java Applet. For example, if Conway-Elkies-Martin compute the effect of the move-sequence

$$0-11-7-9-8-3-0$$

(read from left to right) then we first have to translate this via the dictionary to the move-sequence [0-3-8-2-6-5-0]. Then, we perform this sequence in the Java-applet (note again : a basic move is indicated by the label of the point to click on NOT the counter) and record the final position.

Below we depict the final positions for the three move-sequences [0-3-8-2-6-5-0], [0-9-1-2-0-5-6-12-0] and [0-1-8-0-5-4-0-1-8-0] which are our translations of the three basic move-sequences on page 9 of the CEM-paper (from left to right).



This gives us three reachable positions having their hole at the top. They correspond to the following permutations in the symmetric group S_{12} (from left to right)

$\alpha = (1,10,8,7,2,6,5,3,11,12,4), \beta = (1,9)(2,11)(3,7)(4,10)(5,12)(6,8)$

$\gamma = (2,6)(3,11)(5,8)(10,12)$

Using GAP (or the arithmetic progression loop description of M_{12} as given in Chp.11 section 18 of Conway-Sloane modulo relabeling) we find that the group generated by these three elements is simple and of order 95040 and is isomorphic to the sporadic Mathieu group M_{12}.

This corresponds to the messy part of the 15-puzzle in which we had to find enough reachable positions to generate A_{15}. The more conceptual part (the OXO-labeling showing that all positions must belong to A_{15}) also has a counterpart here. But, before we can tell that story we have to get into linear codes and in particular the properties of the *tetra-code*...

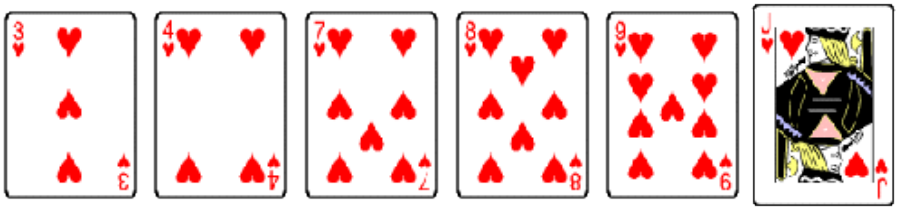
Reference : John H. Conway, Noam D. Elkies and Jeremy L. Martin "The Mathieu Group M_{12} and its pseudogroup extension M_{13}"

1.7 Mathieu's blackjack (1/3)

Mathieu's blackjack is a two-person combinatorial game played with 12 cards of values 0,1,2,...,11. For example take from any deck the numbered cards together with the jack (value 11) and the queen (value 0) (btw. if you find this PI by all means replace the queen by a zero-valued king). Shuffle the cards and divide them into two piles of 6 cards (all of them face up on the table) : the *main-pile* and the *other-pile*. The rules of the game are

- players alternate moves
- a move consists of exchanging a card of the main-pile with a lower-valued card from the other-pile
- the player whose move makes the sum of all cards in the main-pile under 21 looses the game

For example, the starting main-pile might consist of the six cards



This pile has total value 3+4+7+8+9+11=42. A move replaces one of these cards with a lowev valued one not in the pile. So for example, replacing 8 with 5 or 1 or 2 or the queen are all valid moves. A winning move from this situation is for example replacing 8 by the queen (value 0) decreasing the value from 42 to 34

But there are otthers, such as replacing 11 by 5, 9 by 1 or 4 by 2. To win this game you need to know the secrets of the *tetracode* and the *MINIMOG*.

The tetracode is a one-error correcting code consisting of the following nine words of length four over $\mathbb{F}_3 = 0, +, -$

$$\begin{array}{lll} 0\,000 & 0\,++{+} & 0\,--| \\ +\,0\,+\,- & +\,+\,-0 & +\,-\,0+ \\ -\,0\,-\,+ & -\,+\,0- & -\,-\,+0 \end{array}$$

The first element (which is slightly offset from the rest) is the *slope* s of the words, and the other three digits cyclically increase by s (in the field $\mathbb{F}_3$). Because the Hamming-distance is 3 (the minimal number of different digits between two codewords), the tetracode can correct one error, meaning that if at most one of the four digits gets distorted by the channel one can detect and correct this. For example, if you would receive the word $+\ +\,+-$ (which is not a codeword) and if you would know that at most one digits went wrong, you can deduce that the word $+\ 0\ +\ -$ was sent. Thus, one can solve the *4-problem* for the tetracode : correct a tetra-codeword given all 4 of its digits, one of which may be mistaken.

Another easy puzzle is the *2-problem* for the tetra-code : complete a tetra-codeword from any 2 of its digits. For example, given the incomplete word ? ?0+ you can decide that the slope should be + and hence that the complete word must be $+\ -\,0+$.

We will use the MINIMOG here as a way to record the blackjack-position. It is a 4×3 array where the 12 boxes correspond to the card-values by the following scheme

6	3	0	9
5	2	7	10
4	1	8	11

and given a blackjack-position we place a star in the corresponding box, so the above start-position (resp. after the first move) corresponds to

	*		*
		*	
*		*	*
−	0	0	+

respectively

	*	*	*
		*	
*			*
−	0	−	+

In the final row we have added elements of $\mathbb{F}_3$ indicating wher ethe stars are placed in that column (if there is just one star, we write the row-number of the star (ordered 0,+,- from top to bottom), if there are two stars we record the row-number of the empty spot. If we would have three or no stars in a column we would record a wild-card character : ?

Fig. 1.3: Jacob Steiner

Observe that the final row of the start position is $-\ 00+$ which is NOT a tetracodeword, whereas that of the winning position $-\ 0-+$ IS a tetra-codeword! This is the essence of the *Conway-Ryba winning strategy* for Mathieu's blackjack. There are precisely 132 winning positions forming the Steiner-system S(5,6,12).

By an S(5,6,12) we mean a collection of 6-element subsets (our card-piles) from a 12-element set (the deck minus the king) having the amazing property that for EVERY 5-tuple from the 12-set there is a UNIQUE 6-element set containing this 5-tuple. Hence, there are exactly $\binom{12}{5}/6 = 132$ elements in a Steiner S(5,6,12) system. The winning positions are exactly those MINIMOGs having 6 stars such that the final row is a tetra-codeword (or can be extended to a tetra-codeword replacing the wild-cards ? by suitable digits) and such that the distribution of the stars over the columns is NOT (3,2,1,0) in any order.

Provided the given blackjack-position is not in this Steiner-system (and there is only a 1/7 chance that it is), the strategy is clear : remove one of the stars to get a 5-tuple and determine the unique 6-set of the Steiner-system containing this 5-tuple. If the required extra star corresponds to a value less than the removed star you have a legal and winning move (if not, repeat this for another star). Finding these winning positions means solving 2- and 4-problems for the tetracode. In the next section we will say more about this Steiner system and indicate the relation with the Mathieu group M_{12}.

References :

1. J.H. Conway and N.J.A. Sloane, 'The Golay codes and the Mathieu groups', chp. 10 of "Sphere Packings, Lattices and Groups"
2. David Joyner and Ann Casey-Luers, 'Kittens, S(5,6,12) and Mathematical blackjack in SAGE'

1.8 Mathieu's blackjack (2/3)

Take twelve cards and give them values 0,1,2,...,11 (for example, take the jack to have value 11 and the queen to have value 0). The *hexads* are 6-tuples of cards having the following properties.

When we *star* their values by the scheme on the left below and *write* a 0 below a column if it has just one star at the first row or two stars on rows two and three (a + if the unique star is at the first row or two stars in the other columns, and a - if the unique star in on the second row or two stars in rows one and two) or a ? if the column has 3 or 0 stars, we *get* a tetra-codeword (as in the previous section) where we are allowed to replace a ? by any digit. Moreover, we want that the stars are NOT distributed over the four columns such that all of the possible outcomes 0,1,2,3 appear once. For example, the card-pile [queen, 3, 4, 7, 9, jack] is an hexad as is indicated on the right below and has column-distributions (1,1,2,2).

6	3	0	9
5	2	7	10
4	1	8	11

	*	*	*
		*	
*			*
−	0	−	+

The hexads form a Steiner-system S(5,6,12), meaning that every 5-pile of cards is part of a *unique* hexad. The permutations on these twelve cards, having the property that they send every hexad to another hexad, form the sporadic simple group M_{12}, the *Mathieu group* of order 95040.

For now, we assume these facts and deduce from them the *Conway-Ryba winning strategy* for *Mathieu's blackjack* : the hexads are exactly the winning positions and from a non-hexad pile of total value at least 21 there is always a legal (that is, total value decreasing) move to an hexad by replacing one card in the pile by a card from the complement.

It seems that the first proof of this strategy consisted in calculating the Grundy values of all 905 legal positions in Mathieu's blackjack. Later Joseph Kahane and Alex Ryba gave a more conceptual proof, that we will try to understand.

Take a non-hexad 6-pile such that the total value of its cards is at least 21, then removing any one of the six cards gives a 5-pile and is by the Steiner-property contained in a unique hexad. Hence we get 6 different hexads replacing one card from the non-hexad pile by a card not contained in it. We claim that at least one of these operations is a legal move, meaning that the total value of the cards decreases. Let us call a counterexample a *misfit* and record some of its properties until we can prove its non-existence.

A misfit is a non-hexad with total value at least 21 such that all 6 hexads, obtained from it by replacing one card by a card from its complement, have greater total value

A misfit *must contain the queen-card*. If not, we could get an hexad replacing one misfit-card (value ¿ 0) by the queen (value zero) so this would be a legal move. Further, the misfit *cannot contain the jack-card* for otherwise replacing it by a lower-valued card to obtain an hexad is a legal move.

A misfit contains *at least three cards from [queen,1,2,3,4]*. If not, three of these cards are the replacements of misfit-cards to get an hexad, but then at least one of the replaced cards has a greater value than the replacement, giving a legal move to an hexad.

A misfit contains *more than three cards from [queen=0, 1,2,3,4]*. Assume there are precisely three $\{c_1, c_2, c_3\}$ from this set, then the complement of the misfit in the hexad [queen,1,2,3,4,jack] consists of three elements $\{d_1, d_2, d_3\}$ (a misfit cannot contain the jack). The two leftmost columns of the value-scheme (left above) form the hexad 1,2,3,4,5,6 and because the Mathieu group acts 5-transitively there is an element of M_{12} taking $\{0, 1, 2, 3, 4, 11\} \to \{1, 2, 3, 4, 5, 6\}$ and we may even assume that it takes $\{c_1, c_2, c_3\} \to \{4, 5, 6\}$. But then, in the new value-scheme (determined by that M_{12}-element) the two leftmost columns of the misfit look like

*	.	?	?
*	.	?	?
*	.	?	?
?	?		

and the column-distribution of the misfit must be either (3,0,2,1) or (3,0,1,2) (it cannot be (3,0,3,0) or (3,0,0,3) otherwise the (image of the) misfit would be an hexad). Let i,j be the two misfit-values in the 2-starred column. Replacing either of them to get an hexad must have the replacement lying in the second column (in order to get a valid column distribution

(3,1,1,1)). Now, the second column consists of two small values (from [0,1,2,3,4]) and the large jack-value (11). So, at least one of [i,j] is replaced by a smaller valued card to get an hexad, which cannot happen by the misfit-property.

Now, if the misfit shares four cards with queen,1,2,3,4 then *it cannot contain the 10-card*. Otherwise, the replacement to get an hexad of the 10-card must be the 11-card (by the misfit-property) but then there would be another hexads containing five cards from [queen,0,1,2,3,jack] which cannot happen by the Steiner-property. Right, let's summarize what we know so far about our misfit. Its value-scheme looks like

6	III	$*$	9
5	II	7	.
IV	I	8	.

and it must contain three of the four Romans. At this point Kahane and Ryba claim that the two remaining cards (apart from the queen and the three romans) must be such that there is *exactly one from [5,6] and exactly one from [7,8,9]*. They argue this follows from duality where the dual pile of a card-pile $\{x_1, x_2, \ldots, x_6\}$ is the pile $\{11 - x_1, 11 - x_2, \ldots, 11 - x_6\}$. This duality acts on the hexads as the permutation $(0, 11)(1, 10)(2, 9)(3, 8)(4, 7)(5, 6) \in M_{12}$. Still, it is unclear to me how they deduce from it the above claim (lines 13-15 of page 4 of their paper). I'd better have some coffee and work around this in the next section.

If you want to play around a bit with hexads and the blackjack game, you'd better first download SAGE (if you haven't done so already) and then get David Joyner's hexad.sage file and put it in a folder under your sage installation (David suggests 'spam' himself...).

You can load the routines into sage by typing from the sage-prompt *attach 'spam/hexad.sage'*. Now, you can find the hexad from a 5-pile via the command *find-hexad([a1,a2,a3,a4,a5],minimog-shuffle)* and you can get the winning move for a blackjack-position via *blackjack-move([a1,a2,a3,a4,a5,a6],minimog-shuffle)'* (replace - by underscore). More details are in the Joyner-Casey(Luers) paper referenced in the previous section.

Reference : Joseph Kahane and Alexander J. Ryba, 'The hexad game'

1.9 Mathieu's blackjack (3/3)

We are trying to disprove the existence of *misfits*, that is, of non-hexad positions having a total value of at least 21 such that every move to a hexad would increase the total value. So far, we succeeded in showing that such a misfit must have the pattern

6	III	$*$	9
5	II	7	.
IV	I	8	.

That is, a misfit must contain the 0-card (queen) and cannot contain the 10 or 11(jack) and must contain 3 of the four Romans. Now we will see that a misfit also contains precisely one of [5,6] (and consequently also exactly one card from [7,8,9]). To start, it is clear that it cannot contain BOTH 5 and 6 (then its total value can be at most 20). So we have to disprove that a misfit can miss [5,6] entirely (and so the two remaining cards (apart from the zero and the three Romans) must all belong to [7,8,9]).

Lets assume the misfit misses 5 and 6 and does not contain 9. Then, it must contain 4 (otherwise, its column-distribution would be (0,3,3,0) and it would be a hexad). There are just three such positions possible

.	*	*	.
.	*	*	.
*	.	*	.
−	−	?	?

.	*	*	.
.	.	*	.
*	*	*	.
−	+	?	?

.	.	*	.
.	*	*	.
*	*	*	.
−	0	?	?

Neither of these can be misfits though. In the first one, there is an 8-¿5 move to a hexad of smaller total value (in the second a 7-¿5 move and in the third a 7-¿6 move). Right, so the 9 card must belong to a misfit. Assume it does not contain the 4-card, then part of the misfit looks like (with either a 7- or an 8-card added)

.	*	*	*
.	*	?	.
.	*	?	.

contained in the unique hexad

*	*	*	*
.	*		.
.	*		.

Either way the moves 7-¿6 or 8-¿6 decrease the total value, so it cannot be a misfit. Therefore, a misfit must contain both the 4- and 9-card. So it is of the form on the left below

.	?	*	*
.	?	?	.
*	?	?	.

.	.	*	.
.	*	*	*
*	*	.	.
−	0	−	+

.	.	*	*
.	*	*	.
*	*	.	.

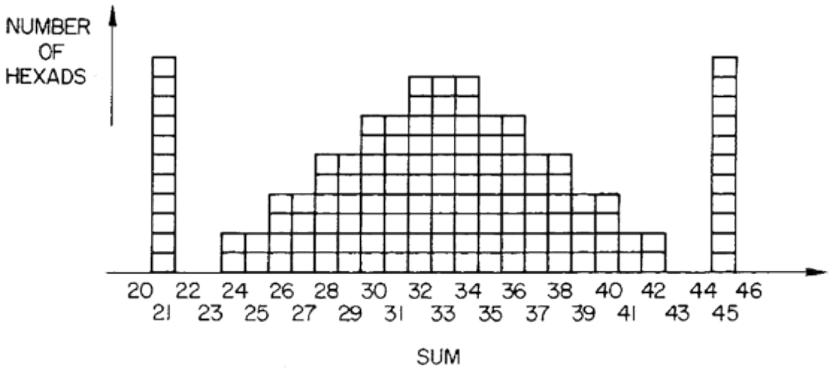
If this is a genuine misfit only the move 9-¿10 to a hexad is possible (the move 9-¿11 is not possible as all BUT ONE of [0,1,2,3,4] is contained in the misfit). Now, the only hexad containing 0,4,10 and 2 from [1,2,3] is in the middle, giving us what the misfit must look like before the move, on the right. Finally, this cannot be a misfit as the move 7-¿5 decreases the total value.

That is, we have proved the claim that a misfit must *contain one of [5,6] and one of [7,8,9]*. Right, now we can deliver the elegant finishing line of the Kahane-Ryba proof. A misfit must contain 0 and three among [1,2,3,4] (let us call the missing card s), one of $5+\epsilon$ with $0 \leq \epsilon \leq 1$ and one of $7+\delta$ with $0 \leq \delta \leq 2$. Then, the total value of the misfit is

$$(0+1+2+3+4-s)+(5+\epsilon)+(7+\delta) = 21+(1+\delta+\epsilon-s)$$

So, if this value is strictly greater than 21 (and we will see in a moment is has to be if it is at least 21) then we deduce that $s < 1+\delta+\epsilon \leq 4$. Therefore $1+\delta+\epsilon$ belongs to the misfit. But then the move $1+\delta\epsilon \to s$ moves the misfit to a 6-tuple with total value 21 and hence (as we see in a moment) must be a hexad and hence this is a decreasing move! So, finally, there are no misfits!

Hence, from every non-hexad pile of total value at least 21 we have a legal move to a hexad. Because the other player cannot move from an hexad to another hexad we are done with our strategy provided we can show (a) that the total value of any hexad is at least 21 and (b) that ALL 6-piles of total value 21 are hexads. As there are only 132 hexads it is easy enough to have their sum-distribution. Here it is



That is, (a) is proved by inspection and we see that there are 11 hexads of sum 21 (the *light hexads* in Conway-speak) and there are only 11 ways to get 21 as a sum of 6 distinct numbers from [0,1,..,11] so (b) follows. Btw. the obvious symmetry of the sum-distribution is another consequence of the duality t-¿11-t discussed briefly at the end of the previous section.

Clearly, I'd rather have conceptual proofs for all these facts and briefly tried my hand. Luckily I did spot the following phrase on page 326 of Conway-Sloane (discussing the above distribution) :

"It will not be easy to explain all the above observations. They are certainly connected with hyperbolic geometry and with the 'hole' structure of the Leech lattice."

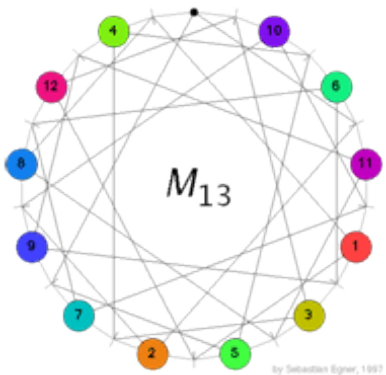
So, I'd better leave it at this...

References :

Joseph Kahane and Alexander J. Ryba, The hexad game"

John H. Conway and N. J.A. Sloane, "Sphere packings, Lattices and Groups" chp. 11 'The Golay codes and the Mathieu groups'

1.10 Conway's M_{13} groupoid (2/2)



Conway's puzzle M_{13} involves the 13 points and 13 lines of $\mathbb{P}^2(\mathbb{F}_3)$. On all but one point numbered counters are placed holding the numbers 1,...,12 and a move involves interchanging one counter and the 'hole' (the unique point having no counter) and interchanging the counters on the two other points of the line determined by the first two points. In the picture on the left, the lines are represented by dashes around the circle in between two counters and the points lying on this line are those that connect to the dash either via a direct line or directly via the circle. In 1.6 we saw that the group of all reachable positions in Conway's M_{13} puzzle 1.3 having the hole at the top positions contains the sporadic simple Mathieu group M_{12} as a subgroup.

To see the reverse inclusion we have to recall the definition of the ternary Golay code named in honor of the Swiss engineer Marcel Golay who discovered in 1949 the binary Golay code that we will encounter *later on*.

The ternary Golay code $\mathcal{C}_{12}$ is a six-dimenional subspace in $\mathbb{F}_3^{\oplus 12}$ and is spanned by its codewords of weight six (the Hamming distance of $\mathcal{C}_{12}$ whence it is a two-error correcting code). There are $264 = 2 \times 132$ weight six codewords and they can be obtained from the 132 *hexads*, we encountered before as the winning positions of Mathieu's blackjack, by replacing the stars by signs + or - using the following rules. By a *tet* (from tetra-codeword) we mean a 3x4 array having 4 +-signs indicating the row-positions of a tetra-codeword. For example

	+		
+		+	
			+
+	0	+	−

is the tet corresponding to the bottom-tetra-codeword.

A *col* is an array having +-signs along one of the four columns. The *signed hexads* will now be the hexads that can be written as $\mathbb{F}_3$ vectors as (depending on the column-distributions of the stars in the hexad indicated between brackets)

$$col-col\ (3^2 0^2) \qquad \pm(col+tet)\ (31^3) \qquad tet-tet\ (2^3 0) \qquad \pm(col+col-tet)\ (2^2 1^2)$$

For example, the hexad on the right has column-distribution $2^3 0$ so its signed versions are of the form tet-tet. The two tetracodewords must have the same digit (-) at place four (so that they cancel and leave an empty column). It is then easy to determine these two tetracodewords giving the signed hexad (together with its negative, obtained by replacing the order of the two codewords)

*	*		
*		*	
	*	*	
−	+	0	−

signed as

+			
	+	+	+
0	−	−	−

−

	+		
+		+	
			+
+	0	+	−

=

+	−		
−		−	
	+	+	
−	+	0	−

and similarly for the other cases. As Conway and Sloane remark 'This is one of many cases when the process is easier performed than described'.

We have an order two operation mapping a signed hexad to its negative and as these codewords span the Golay code, this determines an order two automorphism of $\mathcal{C}_{12}$. Further, forgetting about signs, we get the Steiner-system $S(5, 6, 12)$ of hexads for which the automorphism group is M_{12} hence the automorphism group op the ternary Golay code is $2.M_{12}$, the unique nonsplit central extension of M_{12}.

Right, but what is the connection between the Golay code and Conway's M_{13}-puzzle which is played with points and lines in the projective plane $\mathbb{P}^2(\mathbb{F}_3)$? There are 13 points $\mathcal{P}$ so let us consider a 13-dimensional vectorspace $X = \mathbb{F}_3^{\oplus 13}$ with basis $x_p \ : \ p \in \mathcal{P}$. That is a vector in X is of the form $\vec{v} = \sum_p v_p x_p$ and consider the 'usual' scalar product $\vec{v}.\vec{w} = \sum_p v_p w_p$ on X. Next, we bring in the lines in $\mathbb{P}^2(\mathbb{F}_3)$.

For each of the 13 lines l consider the vector $\vec{l} = \sum_{p \in l} x_p$ with support the four points lying on l and let $\mathcal{C}$ be the subspace (code) of X spanned by the thirteen vectors $\vec{l}$. Vectors $\vec{c}, \vec{d} \in \mathcal{C}$ satisfy the remarkable identity $\vec{c}.\vec{d} = (\sum_p c_p)(\sum_p d_p)$. Indeed, both sides are bilinear in $\vec{c}, \vec{d}$ so it suffices to check teh identity for two line-vectors $\vec{l}, \vec{m}$. The right hand side is then $4.4 = 16 = 1 \bmod 3$ which equals the left hand side as two lines either intersect in one

point or are equal (and hence have 4 points in common). The identity applied to $\vec{c} = \vec{d}$ gives us (note that the squares in $\mathbb{F}_3$ are 0,1) information about the *weight* (that is, the number of non-zero digits) of codewords in $\mathcal{C}$

$$wt(\vec{c})\ mod(3) = \sum_p c_p^2 = (\sum_p c_p)^2 \in \{0, 1\}$$

Let $\mathcal{C}'$ be the collection of $\vec{c} \in \mathcal{C}$ of weight zero (modulo 3) then one can verify that $\mathcal{C}'$ is the orthogonal complement of $\mathcal{C}$ with respect to the scalar product and that the dimension of $\mathcal{C}$ is seven whereas that of $\mathcal{C}'$ is six. Now, let for a point p be $\mathcal{G}_p$ the restriction of

$$\mathcal{C}_p = \{c \in \mathcal{C} \mid c_p = -\sum_{q \in \mathcal{P}} c_q\}$$

to the coordinates of $\mathcal{P} - \{p\}$, then $\mathcal{G}_p$ is clearly a six dimensional code in a 12-dimensional space. A bit more work shows that $\mathcal{G}_p$ is a self-dual code with minimal weight greater or equal to six, whence it must be the ternary Golay code! Now we are nearly done. *Next time* we will introduce a reversi-version of M_{13} and use the above facts to deduce that the basic group of the Mathieu-groupoid indeed is the sporadic simple group M_{12}.

References :

Robert L. Griess, "Twelve sporadic groups" chp. 7 'The ternary Golay code and $2.M_{12}$'

John H. Conway and N. J.A. Sloane, "Sphere packings, lattices and groups" chp 11 'The Golay codes and the Mathieu groups'

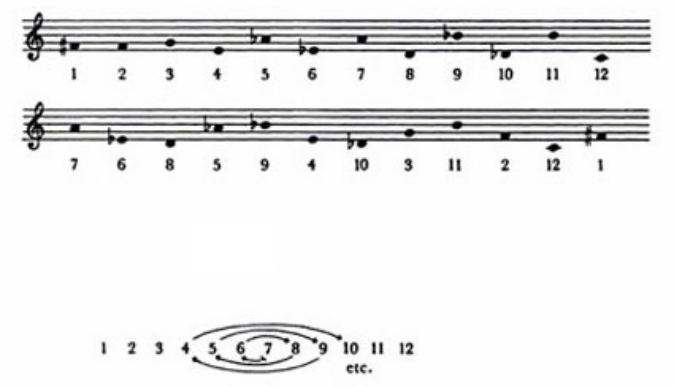
John H. Conway, Noam D. Elkies and Jeremy L. Martin, 'The Mathieu group M_{12} and its pseudogroup extension M_{13}' arXiv:math.GR/0508630

1.11 Olivier Messiaen and Mathieu 12

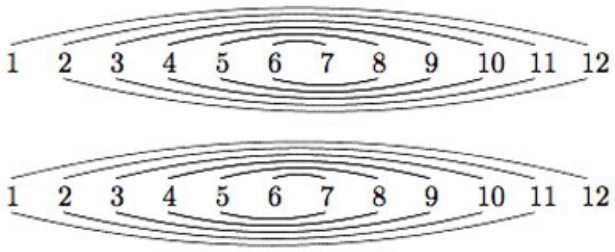
Remember from *the Bourbaki-code booklet* that we identified Olivier Messiaen as the 'Monsieur Modulo' playing the musical organ at the *Bourbaki wedding*. This was based on the fact that his modes transposition limite are really about epimorphisms between modulo rings $\mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$.

However, Messiaen had more serious mathematical tricks up his sleeve. In two of his compositions he did discover (or at least used) one of the smaller sporadic groups, the Mathieu group M_{12} of order 95040 on which we have based the series of Conway's M_{13}-game.

Messiaen's 'Ile de fey 2' composition for piano (part of Quatre tudes de rythme ("Four studies in rhythm"), piano (194950)) is based on two concurrent permutations. The first is shown below, with the underlying motive rotational permutation shown.



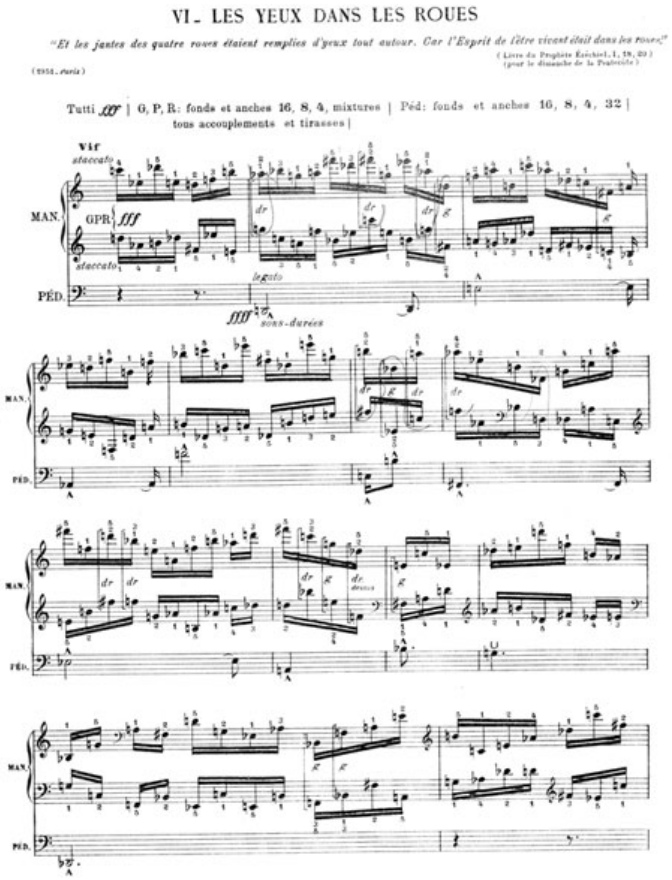
This gives the permutation $(1,7,10,2,6,4,5,9,11,12)(3,8)$. A second concurrent permutation is based on the permutation $(1,6,9,2,7,3,5,4,8,10,11)$ and both of them generate the Mathieu group M_{12}. This can be seen by realizing the two permutations as the rotational permutations



and identifying them with the Mongean shuffles generating M_{12}. See for example, Dave Benson's book "Music: A Mathematical Offering", freely available online.

Clearly, Messiaen doesn't use all of its 95040 permutations in his piece! Here's how it sounds. The piece starts 2 minutes into the clip.

The second piece is "Les Yeux dans les Roues" (The Eyes in the Wheels), sixth piece from the "Livre d'Orgue" (1950/51).



According to Hauptwerk, the piece consists of a melody/theme in the pedal, accompanied by two fast-paced homorhythmic lines in the manuals. The pedal presents a sons-dures

theme which is repeated six times, in different permutations. Initially it is presented in its natural form. Afterwards, it is presented alternatively picking notes from each end of the original form. Similar transformations are applied each time until the sixth, which is the retrograde of the first. The entire twelve-tone analysis (pitch only, not rhythm) of the pedal is shown below:

	D	E	A♭	F	C	B	F♯	E♭	A	B♭	G	D♭
sons-durées	1	2	3	4	5	6	7	8	9	10	11	12
sons-durées, repris des extrêmes au centre	1	3	5	7	9	11	12	10	8	6	4	2
sons-durées, repris des extrêmes au centre, par mouvement rétrograde	2	4	6	8	10	12	11	9	7	5	3	1
sons-durées, repris du centre aux extrêmes, par mouvement rétrograde	12	10	8	6	4	2	1	3	5	7	9	11
sons-durées, repris du centre aux extrêmes	11	9	7	5	3	1	2	4	6	8	10	12
sons-durées, repris par mouvement rétrograde	12	11	10	9	8	7	6	5	4	3	2	1

That is we get the following five permutations which again generate Mathieu 12 :

- $a = (2, 3, 5, 9, 8, 10, 6, 11, 4, 7, 12)$
- $b = (1, 2, 4, 8, 9, 7, 11, 3, 6, 12)(5, 10) = e * a$
- $c = (1, 12, 11, 9, 5, 4, 6, 2, 10, 7)(3, 8) = e * d$
- $d = (1, 11, 10, 8, 4, 5, 3, 7, 2, 9, 6)$
- $e = (1, 12)(2, 11)(3, 10)(4, 9)(5, 8)(6, 7)$

Here's the piece performed on organ.

Considering the permutations $X = d.a^{-1}$ and $Y = (a.d^2.a.d^3)^{-1}$ one obtains canonical generators of M_{12}, that is, generators satisfying the defining equations of this sporadic group

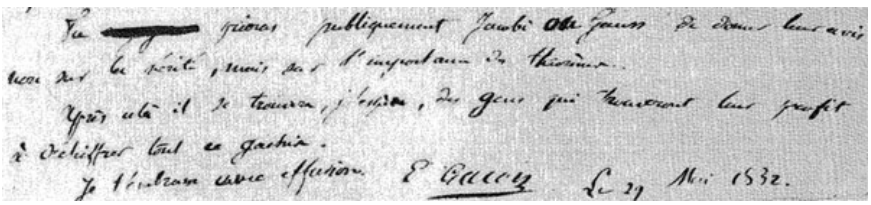
$$X^2 = Y^3 = (XY)^{11} = [X, Y]^6 = (XYXYXY^{-1})^6 = 1$$

I leave you to work out the corresponding *dessin d'enfant* (see the second part).

1.12 Galois' last letter

"Ne pleure pas, Alfred ! J'ai besoin de tout mon courage pour mourir vingt ans!"

We all remember the last words of Evariste Galois to his brother Alfred. Lesser known are the mathematical results contained in his last letter, written to his friend Auguste Chevalier, on the eve of his fatal duel. Here the final sentences :



"Tu prieras publiquement Jacobi ou Gauss de donner leur avis non sur la verite, mais sur l'importance des theoremes. Apres cela il se trouvera, j'espere, des gens qui trouvent leur profis a dechiffrer tout ce gachis.

Je t'embrasse avec effusion. E. Galois, le 29 Mai 1832"

A major result contained in this letter concerns the groups $L_2(p) = PSL_2(\mathbb{F}_p)$, that is the group of 2×2 matrices with determinant equal to one over the finite field $\mathbb{F}_p$ modulo its center. $L_2(p)$ is known to be simple whenever $p \geq 5$.

Galois writes that $L_2(p)$ cannot have a non-trivial permutation representation on fewer than $p+1$ symbols whenever $p > 11$ and indicates the transitive permutation representation on exactly p symbols in the three 'exceptional' cases $p = 5, 7, 11$.

Let $\alpha = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and consider for $p = 5, 7, 11$ the involutions on $\mathbb{P}^1_{\mathbb{F}_p} = \mathbb{F}_p \cup \infty$ (on which $L_2(p)$ acts via Moebius transformations)

$\pi_5 = (0, \infty)(1, 4)(2, 3)$

$\pi_7 = (0, \infty)(1, 3)(2, 6)(4, 5)$

$\pi_{11} = (0, \infty)(1, 6)(3, 7)(9, 10)(5, 8)(4, 2)$

(in fact, Galois uses the involution $(0, \infty)(1, 2)(3, 6)(4, 8)(5, 10)(9, 7)$ for $p = 11$), then $L_2(p)$ leaves invariant the set consisting of the p involutions $\Pi = \alpha^{-i}\pi_p\alpha^i \ : \ 1 \leq i \leq p$. After mentioning these involutions Galois merely writes :

" Ainsi pour le cas de $p = 5, 7, 11$, l'equation modulaire s'abaisse au degre p. En toute rigueur, cette reduction n'est pas possible dans les cas plus eleves. "

Alternatively, one can deduce these permutation representation representations from group isomorphisms. As $L_2(5) \simeq A_5$, the alternating group on 5 symbols, $L_2(5)$ clearly acts transitively on 5 symbols.

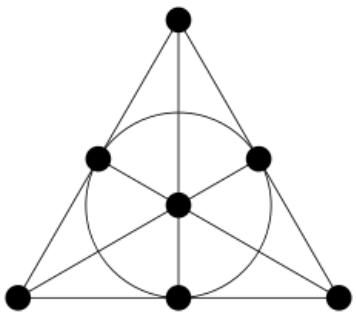


Fig. 1.4: the Fano plane

Similarly, for $p = 7$ we have $L_2(7) \simeq L_3(2)$ and so the group acts as automorphisms on the projective plane over the field on two elements $\mathbb{P}^2_{\mathbb{F}_2}$ aka the Fano plane, depicted on the left.

This finite projective plane has 7 points and 7 lines and $L_3(2)$ acts transitively on them.

For $p = 11$ the geometrical object is a bit more involved. The set of non-squares in $\mathbb{F}_{11}$ is

$\{1, 3, 4, 5, 9\}$

and if we translate this set using the additive structure in $\mathbb{F}_{11}$ one obtains the following 11 five-element sets

$\{1, 3, 4, 5, 9\}, \{2, 4, 5, 6, 10\}, \{3, 5, 6, 7, 11\},$

$\{1, 4, 6, 7, 8\}, \{2, 5, 7, 8, 9\}, \{3, 6, 8, 9, 10\},$

$\{4, 7, 9, 10, 11\}, \{1, 5, 8, 10, 11\}, \{1, 2, 6, 9, 11\},$

$\{1, 2, 3, 7, 10\}, \{2, 3, 4, 8, 11\}$

and if we regard these sets as 'lines' we see that two distinct lines intersect in exactly 2 points and that any two distinct points lie on exactly two 'lines'. That is, intersection sets up a bijection between the 55-element set of all pairs of distinct points and the 55-element set of all pairs of distinct 'lines'. This is called the *biplane geometry*.

The subgroup of S_{11} (acting on the eleven elements of $\mathbb{F}_{11}$) stabilizing this set of 11 5-element sets is precisely the group $L_2(11)$ giving the permutation representation on 11 objects.

An alternative statement of Galois' result is that for $p > 11$ there is no subgroup of $L_2(p)$ *complementary* to the cyclic subgroup

$$C_p = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \; : \; x \in \mathbb{F}_p$$

That is, there is no subgroup such that set-theoretically $L_2(p) = F \times C_p$ (note this is of courese *not* a group-product, all it says is that any element can be written as $g = f.c$ with $f \in F, c \in C_p$.

However, in the three exceptional cases we do have complementary subgroups. In fact, set-theoretically we have

$$L_2(5) = A_4 \times C_5 \qquad L_2(7) = S_4 \times C_7 \qquad L_2(11) = A_5 \times C_{11}$$

and it is a truly amazing fact that the three groups appearing are precisely the three Platonic groups!

Recall that here are 5 Platonic solids coming in three sorts when it comes to rotation-automorphism groups : the tetrahedron (group A_4), the cube and octahedron (group S_4) and the dodecahedron and icosahedron (group A_5). The "4" in the cube are the four body diagonals and the "5" in the dodecahedron are the five inscribed cubes.

That is, our three 'exceptional' Galois-groups correspond to the three Platonic groups, which in turn correspond to the three exceptional Lie algebras E_6, E_7, E_8 via McKay correspondence (wrt. their 2-fold covers). Maybe I'll detail this latter connection another time. It sure seems that surprises often come in triples...

Finally, it is well known that $L_2(5) \simeq A_5$ is the automorphism group of the icosahedron (or dodecahedron) and that $L_2(7)$ is the automorphism group of the Klein quartic.

So, one might ask : is there also a nice curve connected with the third group $L_2(11)$? Rumor has it that this is indeed the case and that the curve in question has genus 70... (to be continued).

bf Reference : Bertram Kostant, "The graph of the truncated icosahedron and the last letter of Galois"

1.13 Arnold's trinities (1/2)

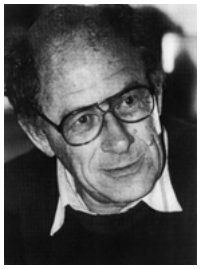


Fig. 1.5: Vladimir Arnold

Referring to the triple of exceptional Galois groups $L_2(5), L_2(7), L_2(11)$ and its connection to the Platonic solids I wrote in the *Galois last letter* section : "It sure seems that surprises often come in triples". Briefly I considered replacing triples by trinities, but then, I didn't want to sound too mystic...

David Corfield of the n-category cafe and a dialogue on infinity (and perhaps other blogs I'm unaware of) pointed me to the paper Symplectization, complexification and mathematical trinities by Vladimir I. Arnold. (here is a PDF-conversion of the paper).

The paper is a write-up of the second in a series of three lectures Arnold gave in june 1997 at the meeting in the Fields Institute dedicated to his 60th birthday. The goal of that lecture was to explain some mathematical dreams he had.

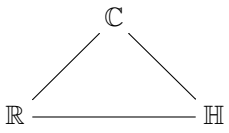
"The next dream I want to present is an even more fantastic set of theorems and conjectures. Here I also have no theory and actually the ideas form a kind of religion rather than mathematics.

The key observation is that in mathematics one encounters many trinities. I shall present a list of examples. The main dream (or conjecture) is that all these trinities are united by some rectangular "commutative diagrams".

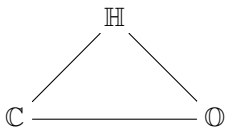
I mean the existence of some "functorial" constructions connecting different trinities. The knowledge of the existence of these diagrams provides some new conjectures which might turn to be true theorems."

Follows a list of 12 trinities, many taken from Arnold's field of expertise being differential geometry. I'll restrict to the more algebraically inclined ones.

1. "The first trinity everyone knows is"

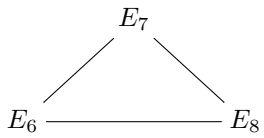


but I would like to alter it into

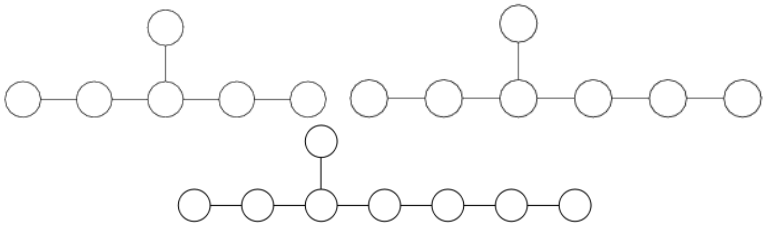


where $\mathbb{H}$ are the Hamiltonian quaternions. The trinity on the left may be natural to differential geometers who see real and complex and hyper-Kaehler manifolds as distinct but related beasts, but I'm willing to bet that most algebraists would settle for the trinity on the right where $\mathbb{O}$ are the octonions.

2. The next trinity is that of the exceptional Lie algebras E6, E7 and E8.



with corresponding Dynkin-Coxeter diagrams

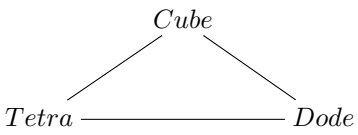


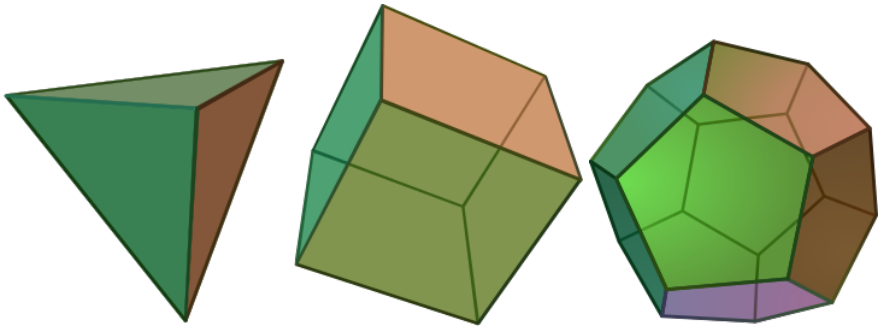
Arnold has this to say about the apparent ubiquity of Dynkin diagrams in mathematics.

" Manin told me once that the reason why we always encounter this list in many different mathematical classifications is its presence in the hardware of our brain (which is thus unable to discover a more complicated scheme). I still hope there exists a better reason that once should be discovered."

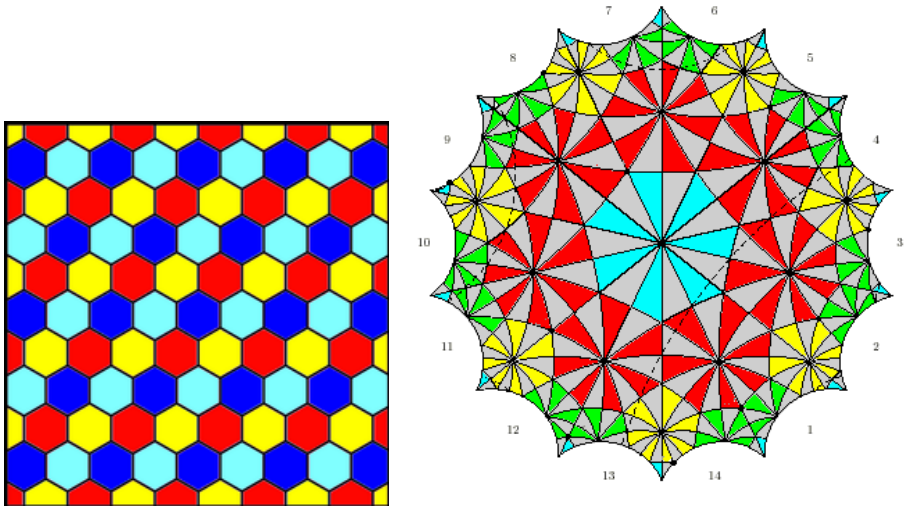
Amen to that. I'm quite hopeful human evolution will overcome some day the limitations of Manin's brain...

3. Next comes the Platonic trinity of the tetrahedron, cube and dodecahedron

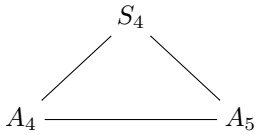




Clearly one can argue against this trinity as follows : a tetrahedron is a bunch of triangles such that there are exactly 3 of them meeting in each vertex, a cube is a bunch of squares, again 3 meeting in every vertex, a dodecahedron is a bunch of pentagons 3 meeting in every vertex... and we can continue the pattern. What should be a bunch a hexagons such that in each vertex exactly 3 of them meet? Well, only one possibility : it must be the hexagonal tiling (on the left below). And in normal Euclidian space we cannot have a bunch of septagons such that three of them meet in every vertex, but in hyperbolic geometry this is still possible and leads to the Klein quartic (on the right). Check out this wonderful post by John Baez for more on this.

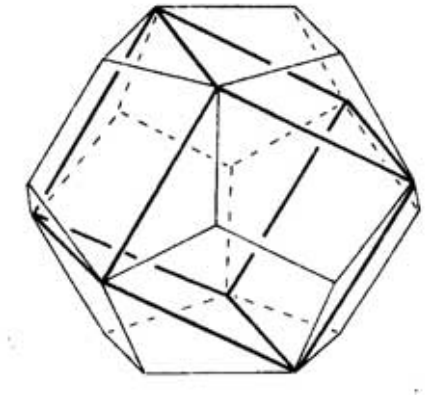


4. The trinity of the rotation symmetry groups of the three Platonics



where A_n is the alternating group on n letters and S_n is the symmetric group.

Clearly, any rotation of a Platonic solid takes vertices to vertices, edges to edges and faces to faces. For the tetrahedron we can easily see the 4 of the group A_4, say the 4 vertices. But what is the 4 of S_4 in the case of a cube? Well, a cube has 4 body-diagonals and they are permuted under the rotational symmetries. The most difficult case is to see the 5 of A_5 in the dodecahedron. Well, here's the solution to this riddle



there are exactly 5 inscribed cubes in a dodecahedron and they are permuted by the rotations in the same way as A_5.

7. The seventh trinity involves complex polynomials in one variable

$$\begin{array}{ccc} & \mathbb{C}[z,z^{-1}] & \\ \swarrow & & \searrow \\ \mathbb{C}[z] & \longrightarrow & \mathbb{C}[z,z^{-1},(z-1)^{-1}] \end{array}$$

the Laurant polynomials and the *modular polynomials* (that is, rational functions with three poles at 0,1 and ∞.

8. The eight one is another beauty

$$\begin{array}{ccc} & TrigonoNumbers & \\ \swarrow & & \searrow \\ Numbers & \longrightarrow & EllipticNumbers \end{array}$$

Here 'numbers' are the ordinary complex numbers $\mathbb{C}$, the 'trigonometric numbers' are the quantum version of those (aka q-numbers) which is a one-parameter deformation and finally, the 'elliptic numbers' are a two-dimensional deformation. If you ever encountered a Sklyanin algebra this will sound familiar.

This trinity is based on a paper of Turaev and Frenkel and I must come back to it some time...

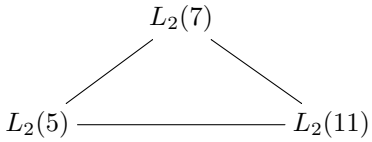
The paper has some other nice trinities (such as those among Whitney, Chern and Pontryagin classes) but as I cannot add anything sensible to it, let us include a few more algebraic trinities. The first one attributed by Arnold to John McKay:

13. A trinity parallel to the exceptional Lie algebra one is

$$\begin{array}{ccc} & 28-biTangents & \\ \swarrow & & \searrow \\ 27-Lines & \longrightarrow & 120-Tritangents \end{array}$$

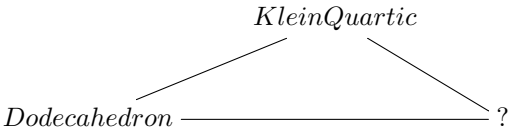
between the 27 straight lines on a cubic surface, the 28 bitangents on a quartic plane curve and the 120 tritangent planes of a canonic sextic curve of genus 4.

14. The exceptional Galois groups



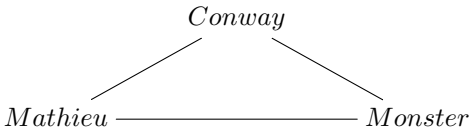
explained in the Galois' last letter section.

15. The associated curves with these groups as symmetry groups



where the ? refers to the mysterious genus 70 curve, now known as the *Buckyball curve*, see the next sections.

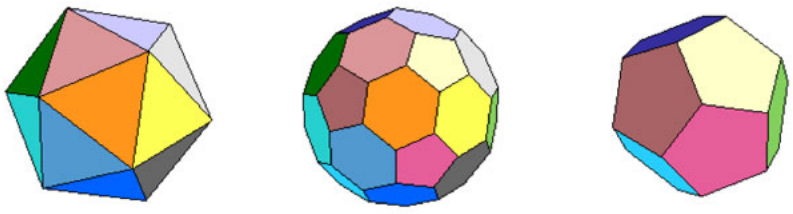
16. The three generations of sporadic groups



Do you have other trinities you'd like to worship?

1.14 The buckyball symmetries

Recall that the buckyball (middle) is a mixed form of two Platonic solids



the Icosahedron on the left and the Dodecahedron on the right.

Let's do some bucky-maths : what is the rotation symmetry group of the buckyball?

For starters, dodeca- and icosahedron are *dual solids*, meaning that if you take the center of every face of a dodecahedron and connect these points by edges when the corresponding faces share an edge, you'll end up with the icosahedron (and conversely). Therefore,

both solids (as well as their mixture, the buckyball) will have the same group of rotational symmetries. Can we at least determine the number of these symmetries?

Take the dodecahedron and fix a face. It is easy to find a rotation taking this face to anyone of its five adjacent faces. In group-slang : the rotation automorphism group acts *transitively* on the 12 faces of the dodecohedron. Now, how many of them fix a given face? These can only be rotations with axis through the center of the face and there are exactly 5 of them preserving the pentagonal face. So, in all we have $12 \times 5 = 60$ rotations preserving any of the three solids above. By composing two of its elements, we get another rotational symmetry, so they form a *group* and we would like to determine what that group is.

There is one group that springs to mind A_5, the subgroup of all *even* permutations on 5 elements. In general, the alternating group has half as many elements as the full permutation group S_n, that is $\frac{1}{2}n!$ (for multiplying with the involution (1,2) gives a bijection between even and odd permutations). So, for A_5 we get 60 elements and we can list them :

- the trivial permutation $()$, being the identity.
- permutations of order two with cycle-decompostion $(i_1, i_2)(i_3, i_4)$, and there are exactly 15 of them around when all numbers are between 1 and 5.
- permutations of order three with cycle-form (i_1, i_2, i_3) of which there are exactly 20.
- permutations of order 5 which have to form one full cycle $(i_1, i_2, i_3, i_4, i_5)$. There are 24 of those.

Can we at least view these sets of elements as rotations of the buckyball? Well, a dodecahedron has 12 pentagobal faces. So there are 4 nontrivial rotations of order 5 for every 2 opposite faces and hence the dodecahedron (and therefore also the buckyball) has indeed 6x4=24 order 5 rotational symmetries.

The icosahedron has twenty triangles as faces, so any of the 10 pairs of opposite faces is responsible for two non-trivial rotations of order three, giving us 10x2=20 order 3 rotational symmetries of the buckyball.

The order two elements are slightly harder to see. The icosahedron has 30 edges and there is a plane going through each of the 15 pairs of opposite edges splitting the icosahedron in two. Hence rotating to interchange these two edges gives one rotational symmetry of order 2 for each of the 15 pairs.

And as 24+20+15+1(identity) = 60 we have found all the rotational symmetries and we see that they pair up nicely with the elements of A_5. But do they form isomorphic groups? In other words, can the buckyball see the *5* in the group A_5.

In the Arnold's trinities section I've shown that one way to see this 5 is as the number of inscribed cubes in the dodecahedron. But, there is another way to see the five based on the order 2 elements described before.

If you look at pairs of opposite edges of the icosahedron you will find that they really come in triples such that the planes determined by each pair are mutually orthogonal (it is best to feel this on ac actual icosahedron). Hence there are 15/3 = 5 such triples of mutually orthogonal symmetry planes of the icosahedron and of course any rotation permutes these triples. It takes a bit of more work to really check that this action is indeed the natural permutation action of A_5 on 5 elements.

Having convinced ourselves that the group of rotations of the buckyball is indeed the alternating group A_5, we can reverse the problem : can the alternating group A_5 *see* the buckyball???

Well, for starters, it can 'see' the icosahedron in a truly amazing way. Look at the conjugacy classes of A_5. We all know that in the full symmetric group S_n elements belong to the same conjugacy class if and only if they have the same cycle decomposition and this is proved using the fact that the conjugation f a cycle $(i_1, i_2, \ldots, i_k)$ under a permutation $\sigma \in S_n$ is equal to the cycle $(\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_k))$ (and this gives us also the candidate needed to conjugate two partitions into each other).

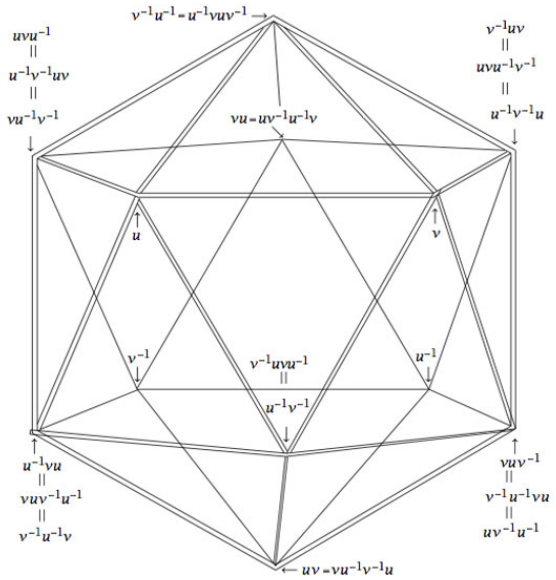
Using this trick it is easy to see that all the 15 order 2 elements of A_5 form one conjugacy class, as do the 20 order 3 elements. However, the 24 order 5 elements split up in two conjugacy classes of 12 elements as the permutation needed to conjugate $(1, 2, 3, 4, 5)$ to $(1, 2, 3, 5, 4)$ is $(4, 5)$ but this is *not* an element of A_5.

Okay, now take one of these two conjugacy classes of order 5 elements, say that of $(1, 2, 3, 4, 5)$. It consists of 12 elements, 12 being also the number of *vertices* of the icosahedron. So, is there a way to identify the elements in the conjugacy class to the vertices in such a way that we can describe the edges also in terms of group-computations in A_5?

Surprisingly, this is indeed the case as is demonstrated in a marvelous paper by Kostant The graph of the truncated icosahedron and the last letter of Galois.

Two elements a, b in the conjugacy class C share an edge if and only if their product $a.b \in A_5$ still belongs to the conjugacy class C! So, for example $(1, 2, 3, 4, 5).(2, 1, 4, 3, 5) = (2, 5, 4)$ so there is no edge between these elements, but on the other hand $(1, 2, 3, 4, 5).(5, 3, 4, 1, 2) = (1, 5, 2, 4, 3)$ so there is an edge between these! It is no coincidence that $(5, 3, 4, 1, 2) = (2, 1, 4, 3, 5)^{-1}$ as inverse elements correspond in the bijection to opposite vertices and for any pair of non-opposite vertices of an icosahedron it is true that either they are neighbors or any one of them is the neighbor of the opposite vertex of the other element.

If we take $u = (1, 2, 3, 4, 5)$ and $v = (5, 3, 4, 1, 2)$ (or any two elements of the conjugacy class such that u.v is again in the conjugacy class), then one can describe all the vertices of the icosahedron group-theoretically as follows



Isn't that nice? Well yes, you may say, but that is just the icosahedron. Can the group A_5 also see the buckyball?

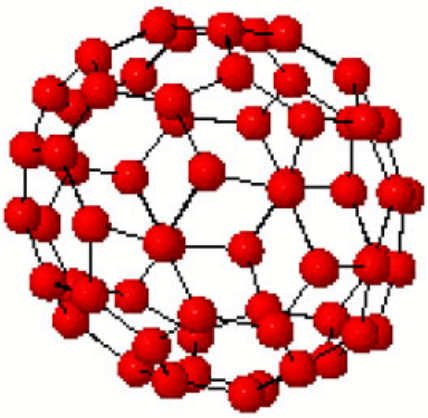
Well, let's try a similar strategy : the buckyball has 60 vertices, exactly as many as there are elements in the group A_5. Is there a way to connect certain elements in a group according to fixed rules? Yes, there is such a way and it is called the Cayley Graph of a group. It goes like this : take a set of generators $g_1, \ldots, g_k$ of a group G, then connect two group element $a, b \in G$ with an edge if and only if $a = g_i.b$ or $b = g_i.a$ for some of the generators.

Back to the alternating group A_5. There are several sets of generators, one of them being the elements $(1,2,3,4,5), (2,3)(4,5)$. In the paper mentioned before, Kostant gives an impressive group-theoretic proof of the fact that the Cayley-graph of A_5 with respect to these two generators is indeed the buckyball!

Let us allow to be lazy for once and let SAGE do the hard work for us, and let us just watch the outcome. Here's how that's done

```
> A=PermutationGroup(['(1,2,3,4,5)','(2,3)(4,5)'])
> B=A.cayley_graph()
> B.show3d()
```

The outcone is a nice 3-dimensional picture of the buckyball. Below you can see a still, and, if you click here you will get a 3-dimensional model of it (first click the 'here' link in the new window and then you'd better control-click and set the zoom to 200

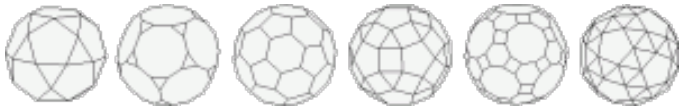


Hence, viewing this Cayley graph from different points we have convinced ourselves that it is indeed the buckyball. In fact, most (truncated) Platonic solids appear as Cayley graphs of groups with respect to specific sets of generators. For later use here is a (partial) survey (taken from Jaap's puzzle page)

- Tetrahedron : $C_2 \times C_2, [(12)(34), (13)(24), (14)(23)]$
- Cube : $D_4, [(1234), (13)]$
- Octahedron : $S_3, [(123), (12), (23)]$

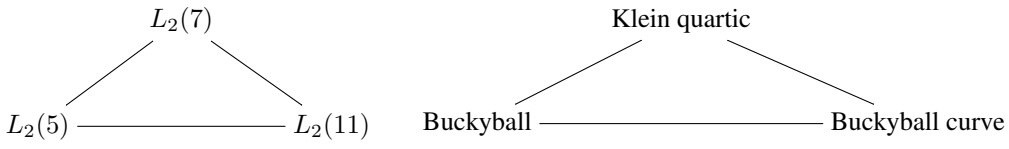
- Dodecahedron : IMPOSSIBLE
- Icosahedron :** $A_4, [(123), (234), (13)(24)]$

- Truncated tetrahedron : $A_4, [(123), (12)(34)]$
- Cuboctahedron : $A_4, [(123), (234)]$
- Truncated cube : $S_4, [(123), (34)]$
- Truncated octahedron : $S_4, [(1234), (12)]$
- Rhombicubotahedron : $S_4, [(1234), (123)]$
- Rhombitruncated cuboctahedron : IMPOSSIBLE
- Snub cuboctahedron : $S_4, [(1234), (123), (34)]$



- Icosidodecahedron : IMPOSSIBLE
- Truncated dodecahedron : $A_5, [(124), (23)(45)]$
- Truncated icosahedron : $A_5, [(12345), (23)(45)]$
- Rhombicosidodecahedron : $A_5, [(12345), (124)]$
- Rhombitruncated icosidodecahedron : IMPOSSIBLE
- Snub Icosidodecahedron : $A_5, [(12345), (124), (23)(45)]$

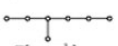
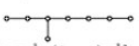
Again, all these statements can be easily verified using SAGE via the method described before. Next time we will go further into the Kostant's group-theoretic proof that the buckyball is the Cayley graph of A_5 with respect to (2,5)-generators as this calculation will be crucial in the description of the *buckyball curve*, the genus 70 Riemann surface discovered by David Singerman and Pablo Martin which completes the trinity corresponding to the Galois trinity (see the Arnold trinities section).



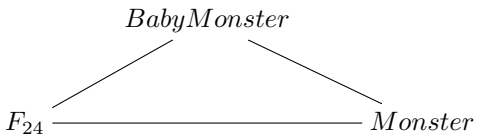
1.15 Arnold's trinities (2/2)

Arnold has written a follow-up to the paper mentioned in the previous section called Polymathematics : is mathematics a single science or a set of arts? (or here for a (huge) PDF-conversion).

On page 8 of that paper is a nice summary of his 25 trinities :

(1)	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{H}$
(2)	Morse theory anses attachment	Picard-Lefschetz theory Dehn twist	?
(3)	$\pi_0(\mathbb{R}\setminus 0)=\mathbb{Z}_2$	$\pi_1(\mathbb{C}\setminus 0)=\mathbb{Z}$	$\pi_3(\mathbb{H}\setminus 0)=\mathbb{Z}$?
(4)	$\mathbb{R}P^n$	$\mathbb{C}P^n$	$\mathbb{H}P^n$
(5)	$\mathbb{R}P^1=S^1$	$\mathbb{C}P^1=S^2$	$\mathbb{H}P^1=S^4$
(6)	$\mathbb{R}P^1/\mathrm{Aut}\mathbb{R}=S^1$	$\mathbb{C}P^2/\mathrm{Aut}\mathbb{C}=S^4$	$\frac{\mathbb{H}P^4/\mathrm{Aut}\mathbb{H}}{\mathrm{Conj}}=S^{13}$
(7)	Quadratic forms	Hermitian forms	Hyperhermitian forms
(8)	Von Neuman Wigner eigenvalues repulsion	Quantum Hall effect and Berry phase	?
(9)	Möbius S^0 bundle $S^1\to S^1$	Hopf S^1 bundle $S^3\to S^2$	Hopf S^3 bundle $S^7\to S^4$
(10)	Monodromy of a covering	Curvature of a connection	Hypercurvature of a hyperconnection?
(11)	w	c	p
(12)	$O,\ SO$	$U,\ SU$	$Sp,\ ?$
(13)	Tetrahedron	Octahedron	Icosahedron
(14)	$(4,4,6)$	$(6,8,12)$	$(12,20,30)$
(15)	$x^2+y^3+z^4$	$x^2+y^3+yz^3$	$x^2+y^3+z^5$
(16)	$x^3+y^3+z^3$	$x^2+y^4+z^4$	$x^2+y^3+z^6$
(17)	$(\pi/3,\pi/3,\pi/3)$	$(\pi/2,\pi/4,\pi/4)$	$(\pi/2,\pi/3,\pi/6)$
(18)	A_3	B_3 	H_3 
(19)	$2(1+3+3+5)=24$	$2(1+5+7+11)=48$	$2(1+11+19+29)=120$
(20)	$(2,4,4,6)$	$(2,6,8,12)$	$(2,12,20,30)$
(21)	D_4 	F_4	H_4 
(22)	E_6 	E_7 	E_8 
(23)	$\mathbb{C}[t]$	$\mathbb{C}[t,t^{-1}]$	$\mathbb{C}[t,t^{-1},(1-t)^{-1}]$
(24)	Numbers	Trigonometric numbers	Elliptic numbers
(25)	H	K	Ell

I learned of this newer paper from a comment by Frederic Chapoton who maintains a nice webpage dedicated to trinities. In Frederic's list there is one trinity on sporadic groups :



where F_{24} is the Fischer simple group of order $2^{21}.3^{16}.5^2.7^3.11.13.17.23.29 = 1255205709190661721292800$, which is the third largest sporadic group (the two larger ones being the Baby Monster and the Monster itself).

I don't know what the rationale is behind this trinity. But I'd like to recall the (Baby)Monster history as a warning against the trinity-reflex. Sometimes, there is just no way to extend a *would be* trinity.

The story comes from Mark Ronan's book Symmetry and the Monster on page 178.

”Let’s remind ourselves how we got here. A few years earlier, Fischer has created his ’transposition’ groups Fi22, Fi23, and Fi24. He had called them M(22), M(23), and M(24), because they were related to Mathieu’s groups M22,M23, and M24, and since he used Fi22 to create his new group of mirror symmetries, he tentatively called it M^{22}.

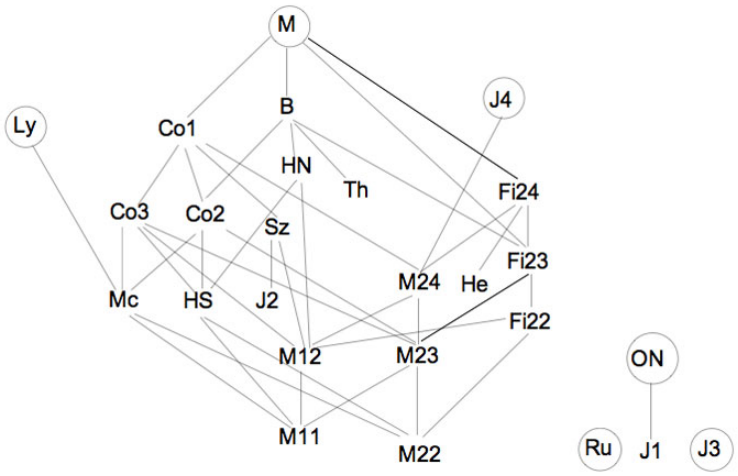
It seemed to appear as a cross-section in something even bigger, and as this larger group was clearly associated with Fi24, he labeled it M^{24}. Was there something in between that could be called M^{23}?

Fischer visited Cambridge to talk on his new work, and Conway named these three potential groups the *Baby Monster*, the *Middle Monster*, and the *Super Monster*. When it became clear that the Middle Monster didn’t exist, Conway settled on the names Baby Monster and Monster, and this became the standard terminology.”

Marcus du Sautoy’s account in Finding Moonshine is slightly different. He tells on page 322 that the Super Monster didn’t exist. Anyone knowing the factual story?

”Some mathematical trickery later revealed that the Super Monster was going to be impossible to build: there were certain features that contradicted each other. It was just a mirage, which vanished under closer scrutiny. But the other two were still looking robust. The Middle Monster was rechristened simply the Monster.”

And, the inclusion diagram of the sporadic simples tells yet another story.



Anyhow, this inclusion diagram is helpful in seeing the three generations of the *Happy Family* (as well as the *Pariahs*) of the sporadic groups, terminology invented by Robert Griess in his 100+p Inventiones paper on the construction of the Monster (which he liked to call, for obvious reasons, the Friendly Giant denoted by FG). The happy family appears in Table 1.1. of the introduction.

Table 1.1. Construction of the happy family[a]

Construct...	then derive existence of...
M_{24}	$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$
0	1, 2, 3, HiS, McL, Suz, HJ
F_1	$F_2, F_3, F_5, F_{22}, F_{23}, F'_{24}$, Held

[a] except possibly for J_1

It was this picture that made me propose the trinity on the left below in the previous section. I now like to add another trinity on the right, and, the connection between the two is clear.

Here $Golay$ denotes the extended binary Golay code of which the Mathieu group M_{24} is the automorphism group. $Leech$ is of course the 24-dimensional Leech lattice of which the automorphism group is a double cover of the Conway group Co_1. $Griess$ is the Griess algebra which is a nonassociative 196884-dimensional algebra of which the automorphism group is the Monster.

I am aware of a construction of the Leech lattice involving the quaternions (the icosian construction of chapter 8, section 2.2 of SPLAG). Does anyone know of a construction of the Griess algebra involving octonions???

1.16 Klein's dessins d'enfants and the buckyball

We saw that the icosahedron can be constructed from the alternating group A_5 by considering the elements of a conjugacy class of order 5 elements as the vertices and edges between two vertices if their product is still in the conjugacy class.

This description is so nice that one would like to have a similar construction for the buckyball. But, the buckyball has 60 vertices, so they surely cannot correspond to the elements of a conjugacy class of A_5. But, perhaps there is a larger group, somewhat naturally containing A_5, having a conjugacy class of 60 elements?

This is precisely the statement contained in *Galois' last letter*. He showed that 11 is the largest prime p such that the group $L_2(p) = PSL_2(\mathbb{F}_p)$ has a (transitive) permutation presentation on p elements. For, $p = 11$ the group $L_2(11)$ is of order 660, so it permuting 11 elements means that this set must be of the form $X = L_2(11)/A$ with $A \subset L_2(11)$ a subgroup of 60 elements... and it turns out that $A \simeq A_5$...

Actually there are TWO conjugacy classes of subgroups isomorphic to A_5 in $L_2(11)$ and we have already seen one description of these using the *biplane geometry* (one class is the stabilizer subgroup of a 'line', the other the stabilizer subgroup of a point).

Here, we will give yet another description of these two classes of A_5 in $L_2(11)$, showing among other things that the theory of dessins d'enfant predates Grothendieck by 100 years.

In the very same paper containing the first depiction of the *Dedekind tessellation* (see the Dedekind or Klein section), Klein found that there should be a degree 11 cover $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ with monodromy group $L_2(11)$, ramified only in the three points $0, 1, \infty$ such that there is just one point lying over ∞, seven over 1 of which four points where two sheets come together and finally 5 points lying over 0 of which three where three sheets come together. In 1879 he wanted to determine this cover explicitly in the paper "Ueber die Transformationen elfter Ordnung der elliptischen Funktionen" (Math. Annalen) by describing all Riemann surfaces with this ramification data and pick out those with the correct monodromy group.

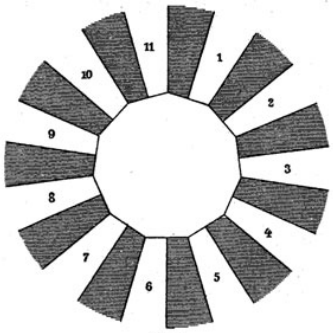


Fig. 1.

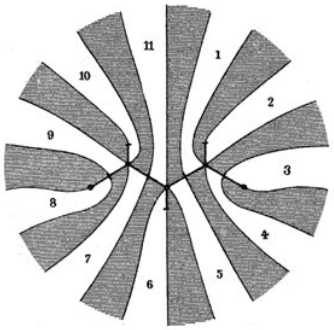


Fig. 3.

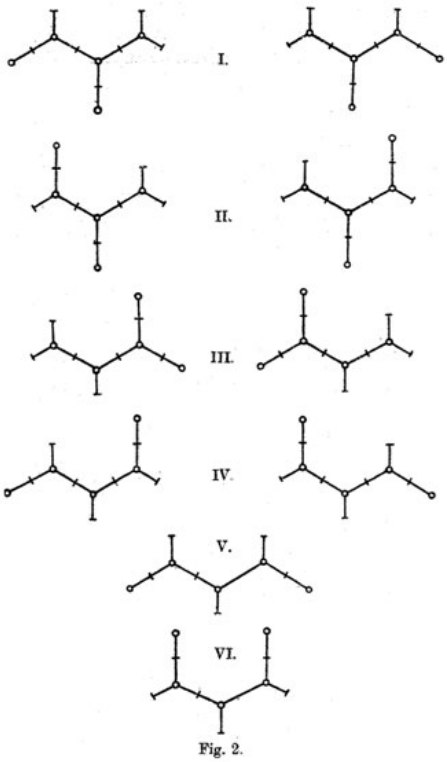


Fig. 2.

He manages to do so by associating to all these covers their 'dessins d'enfants' (which he calls *Linienzuges*), that is the pre-image of the interval [0,1] in which he marks the preimages of 0 by a bullet and those of 1 by a +, such as in the innermost darker graph on the right above.

He even has these two wonderful pictures explaining how the dessin determines how the 11 sheets fit together. (More examples of dessins and the correspondences of sheets were drawn in the 1878 paper.)

The ramification data translates to the following statements about the Linienzuge : (a) it must be a tree (∞ has one preimage), (b) there are exactly 11 (half)edges (the degree of the cover), (c) there are 7 +-vertices and 5 o-vertices (preimages of 0 and 1) and (d) there are 3 trivalent o-vertices and 4 bivalent +-vertices (the sheet-information).

Klein finds that there are exactly 10 such dessins and lists them in his Fig. 2 (left). Then, he claims that one the two dessins of type I give the correct monodromy group. Recall that the *monodromy group* (see the second part) is found by giving each of the half-edges a number from 1 to 11 and looking at the permutation τ of order two pairing the half-edges adjacent to a +-vertex and the order three permutation σ listing the half-edges by cycling counter-clockwise around a o-vertex. The monodromy group is the group generated by these two elements.

For example, if we label the type V-dessin by the numbers of the white regions bordering the half-edges (as in the picture Fig. 3 on the right above) we get $\sigma = (7,10,9)(5,11,6)(1,4,2)$ and $\tau = (8,9)(7,11)(1,5)(3,4)$.

Nowadays, it is a matter of a few seconds to determine the monodromy group using GAP and we verify that this group is A_{11}.

Of course, Klein didn't have GAP at his disposal, so he had to rule out all these cases by hand.

```
> gap> g:=Group((7,10,9)(5,11,6)(1,4,2),(8,9)(7,11)(1,5)(3,4));
> Group([ (1,4,2)(5,11,6)(7,10,9), (1,5)(3,4)(7,11)(8,9) ])
> gap> Size(g);
> 19958400
> gap> IsSimpleGroup(g);
> true
```

Klein used the fact that $L_2(7)$ only has elements of orders 1,2,3,5,6 and 11. So, in each of the remaining cases he had to find an element of a different order. For example, in type V he verified that the element $\tau.(\sigma.\tau)^3$ is equal to the permutation (1,8)(2,10,11,9,6,4,5)(3,7) and consequently is of order 14.

Perhaps Klein knew this but GAP tells us that the monodromy group of all the remaining 8 cases is isomorphic to the alternating group A_{11} and in the two type I cases is indeed $L_2(11)$. Anyway, the two dessins of type I correspond to the two conjugacy classes of subgroups A_5 in the group $L_2(11)$.

But, back to the buckyball! The upshot of all this is that we have the group $L_2(11)$ containing two classes of subgroups isomorphic to A_5 and the larger group $L_2(11)$ does indeed have two conjugacy classes of order 11 elements containing exactly 60 elements (compare this to the two conjugacy classes of order 5 elements in A_5 in the icosahedral construction). Can we construct the buckyball out of such a conjugacy class?

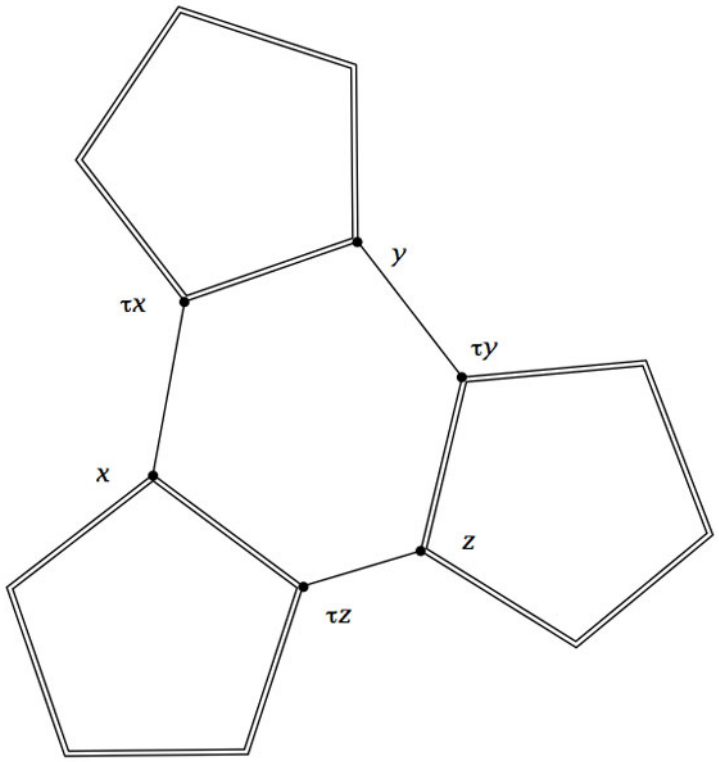
To start, we can identify the 12 pentagons of the buckyball from a conjugacy class C of order 11 elements. If $x \in C$, then so do x^3, x^4, x^5 and x^9, whereas the powers $x^2, x^6, x^7, x^8, x^{10}$ belong to the other conjugacy class. Hence, we can divide our 60 elements in 12 subsets of 5 elements and taking an element x in each of these, the vertices of a pentagon correspond (in order) to (x, x^3, x^9, x^5, x^4).

Group-theoretically this follows from the fact that the factorgroup of the normalizer of x modulo the centralizer of x is cyclic of order 5 and this group acts naturally on the conjugacy class of x with orbits of size 5.

Finding out how these pentagons fit together using hexagons is a lot subtler... and in The graph of the truncated icosahedron and the last letter of Galois Bertram Kostant shows how to do this.

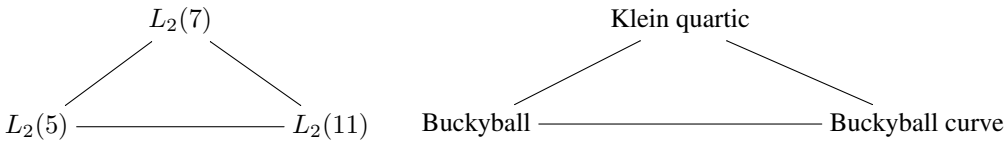
Fix a subgroup isomorphic to A_5 and let D be the set of all its order 2 elements (recall that they form a full conjugacy class in this A_5 and that there are precisely 15 of them). Now, the startling observation made by Kostant is that for our order 11 element x in C there is a *unique* element $a \in D$ such that the commutator $b = [x,a] = x^{-1}a^{-1}xa$ belongs again to D. The unique hexagonal side having vertex x connects it to the element $b.x$which belongs again to C as $b.x = (ax)^{-1}.x.(ax)$.

Concluding, if C is a conjugacy class of order 11 elements in $L_2(11)$, then its 60 elements can be viewed as corresponding to the vertices of the buckyball. Any element $x \in C$ is connected by two pentagonal sides to the elements x^3 and x^4 and one hexagonal side connecting it to $\tau x = b.x$.



1.17 The buckyball curve

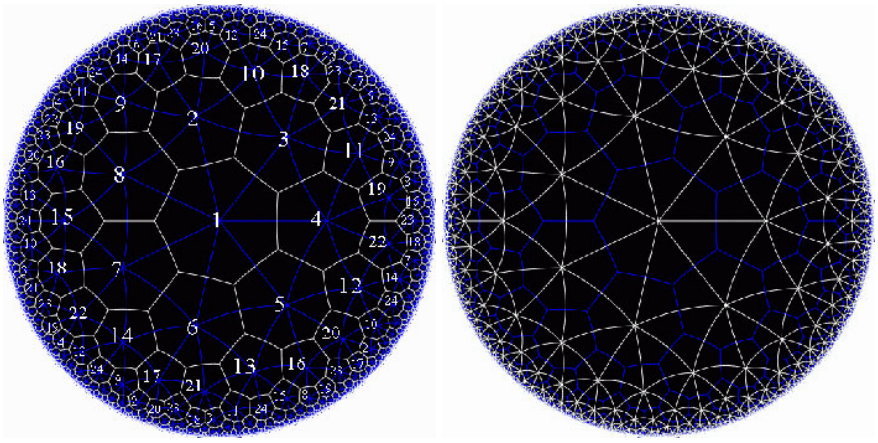
We are after the geometric trinity corresponding to the trinity of exceptional Galois groups



The surfaces on the right have the corresponding group on the left as their group of automorphisms. But, there is a lot more group-theoretic info hidden in the geometry. Before we sketch the $L_2(11)$ case, let us recall the simpler situation of $L_2(7)$.

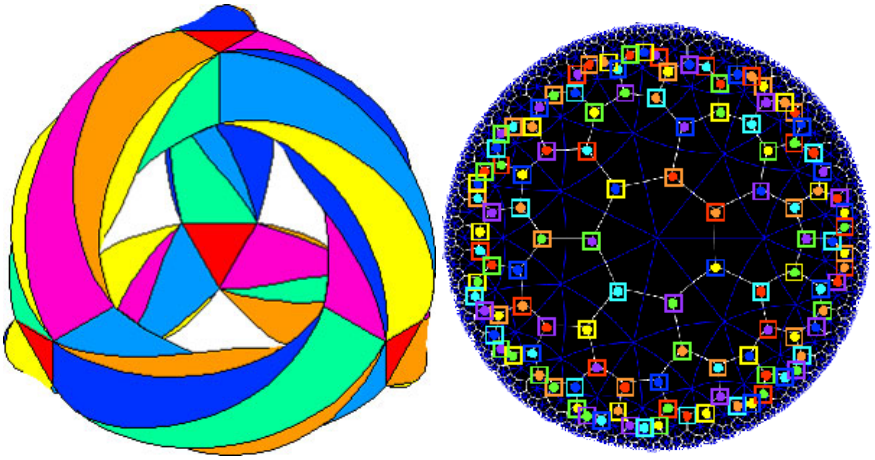
There are some excellent web-page on the Klein quartic and it would be too hard to try to improve on them, so we refer to John Baez' page and Greg Egan's page for more details.

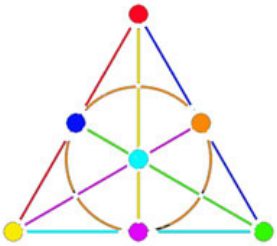
The Klein quartic is the degree 4 projective plane curve defined by the equation $x^3y + y^3z + z^3x = 0$. It can be tiled with a set of 24 regular heptagons, or alternatively with a set of 56 equilateral triangles and these two tilings are dual to each other



In the triangular tiling, there are 56 triangles, 84 edges and 24 vertices. The 56 triangles come in 7 bunches of 8 each and we give the 7 bunches of triangles each a different color as in the pictures below made by Greg Egan. Observe that in the hyperbolic tiling all triangles look alike, but in the picture on the left most of them get warped as we try to embed the quartic in 3-space (which is impossible to do properly). The non-warped triangles (the red ones) come into pairs, the top and bottom triangles of a triangular prism, one prism at each of the four 'vertices' of a tetrahedron.

The automorphism group $L_2(7)$ acts on these triangles as S_4 acts on the triangles in a truncated cube.





The buckyball construction from a conjugacy class of order 11 elements from $L_2(11)$ recalled in the last section, has an analogon $L_2(7)$, leading to the truncated cube.

In $L_2(7)$ there are two conjugacy classes of subgroups isomorphic to S_4 (the rotation-symmetry group of the cube) as well as two conjugacy classes of order 7 elements, each consisting of precisely 24 elements, say C and D. The normalizer subgroup of C has order 21, so there is a cyclic group of order 3 acting non-trivially on the conjugacy class C with 8 orbits consisting of three elements each. These are the eight triangles of the truncated cube identified above as the red triangles.

Shifting perspective, we can repeat this for each of the seven different colors. That is, we have seven truncated cubes in the Klein quartic. On each of them a copy of S_4 acts and these subgroups form one of the two conjugacy classes of S_4 in the group $L_2(7)$. The colors of the triangles of these seven truncated cubes are indicated by bullets in the picture above on the right. The other conjugacy class of S_4's act on 'truncated anti-cubes' which also come in seven bunches of which the color is indicated by a square in that picture.

If you spend enough time on it you will see that each (truncated) cube is completely disjoint from precisely 3 (truncated) anti-cubes. This reminds us of the Fano-plane (picture on the left) : it has 7 points (our seven truncated cubes), 7 lines (the truncated anti-cubes) and the incidence relation of points and lines corresponds to the disjointness of (truncated) cubes and anti-cubes! This is the geometric interpretation of the group-theoretic realization that $L_2(7) \simeq PGL_3(\mathbb{F}_2)$ is the isomorphism group of the projective plane over the finite field $\mathbb{F}_2$ on two elements, that is, the Fano plane. The colors of the picture on the left indicate the colors of cubes (points) and anti-cubes (lines) consistent with Egan's picture above.

Further, the 24 vertices correspond to the 24 cusps of the modular group $\Gamma(7)$. Recall that a modular interpretation of the Klein quartic is as $\mathbb{H}/\Gamma(7)$ where $\mathbb{H}$ is the upper half-plane on which the modular group $\Gamma = PSL_2(\mathbb{Z})$ acts via Moebius transformations, that is, to a 2x2 matrix corresponds the transformation

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad -z\rightarrow \quad \mapsto \frac{az+b}{cz+d}$$

Okay, now let's briefly sketch the exciting results found by Pablo Martin and David Singerman in the paper From biplanes to the Klein quartic and the buckyball, extending the above to the group $L_2(11)$.

There is one important modification to be made. Recall that the *Cayley-graph* to get the truncated cube comes from taking as generators of the group S_4 the set $(3,4),(1,2,3)$, that is, an order two and an order three element, defining an epimorphism from the modular group $\Gamma = C_2 * C_3 \to S_4$.

We have also seen that in order to get the buckyball as a Cayley-graph for A_5 we need to take the generating set $(2,3)(4,5),(1,2,3,4,5)$, so a degree two and a *degree five* element.

Hence, if we want to have a corresponding Riemann surface we'd better not start from the action of the modular group on the upper half-plane, but rather the action via Moebius transformations of the *Hecke group*

$H^5 \simeq C_2 * C_5 = \langle z \mapsto -\frac{1}{z}, z \mapsto z+\phi \rangle$

where $\phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio.

But then, there is an epimorphism $H^5 \to L_2(11)$ (as this group is generated by one element of degree 2 and one of degree 5) and let Λ denote its kernel. Observe that Λ is the analogon of the modular subgroup $\Gamma(7)$ used above to define the Klein quartic.

Hence, Martin and Singerman define the *buckyball curve* as the modular quotient $X = \mathbb{H}/\Lambda$ which is a Riemann surface of genus 70.

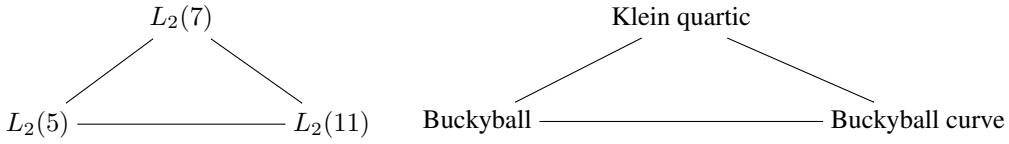
The terminology is motivated by the fact that, precisely as we got 7 truncated cubes in the Klein quartic, we now get 11 truncated icosahedra (that is, buckyballs) in X. The 11 coming, analogous to the Klein case, from the fact that there are precisely two conjugacy classes of subgroups of $L_2(11)$ isomorphic to A_5, each class containing precisely eleven elements! The 60 vertices of the buckyball again correspond to the fact that there are 60 cusps in this case.

So, what is the analogon of the Fano plane in this case? Well, observe that the Fano-plane is a *biplane of order two*. That is, if we take as 'points' the points of the Fano plane and

as 'lines' the complements of lines in the Fano plane then this defines a biplane structure. This means that any two distinct 'points' are contained in two distinct 'lines' and that two distinct 'lines' intersect in two distinct 'points'. A biplane is said to be of order k is each 'line' consist of k-2 'points'. As the complement of a line in the Fano plane consists of 4 points, the Fano plane is therefore a biplane of order 2. The intersection pattern of cubes and anti-cubes in the Klein quartic is this biplane structure on the Fano plane.

In a similar way, Martin and Singerman show that the two conjugacy classes of subgroups isomorphic to A_5 in $L_2(11)$, each containing exactly 11 elements, correspond to 11 embedded buckyballs (and 11 anti-buckyballs) in the buckyball-curve X and that the intersection relations among them describe the combinatorial structure of a biplane of order three if we view the 11 buckys as 'points' and the anti-buckys as 'lines'.

That is, the buckyball curve is a perfect geometric counterpart of the Klein quartic for the two trinities



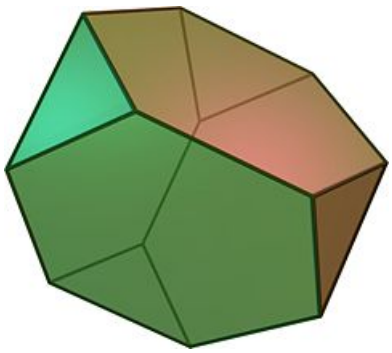
At the Arcadian Functor, Kea also has a post on this in which she conjectures that the Kac-Moody algebra of E11 may be related to the buckyball curve.

References :

David Singerman, "Klein's Riemann surface of genus 3 and regular embeddings of finite projective planes" Bull. London Math. Soc. 18 (1986) 364-370.

Pablo Martin and David Singerman, "From biplanes to the Klein quartic and the Buckyball"

1.18 The "uninteresting" case $p = 5$



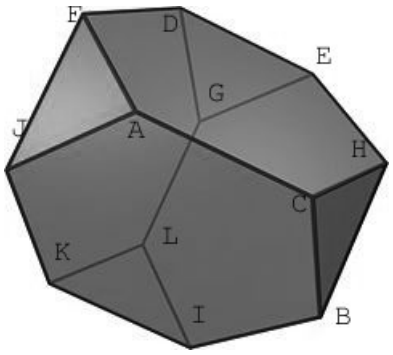
"I was hoping you would write a post on the uninteresting case of p=5 in this context. Note that the truncated tetrahedron has (V,E,F)=(12,18,8) which is a triple that appears in the ternary (cyclic) geometry for the cube. This triple can be 4 hexagons and 4 triangles (the truncated tetrahedron) OR 4 pentagons and 4 squares!" Kea commented and I didnt know the answer to the 'obvious' question : *"how can one get the truncated tetrahedron from either of the two conjugacy classes of order 5 elements in $L_2(5) = A_5$, each consisting of 12 elements"*.

Fortunately the groups involved are small enough to enable hand-calculations. Probably there is a more elegant way to do this, but I was already happy to find this construction...

This time, there is just one conjugacy class of subgroups isomorphic to A_4 (the symmetry group of the (truncated) tetrahedron) in $L_2(5) = A_5$. Take one of the two conjugacy classes C of 5-cycles in A_5 and use the following notation for its 12 elements :

A=(1,2,3,4,5), B=(1,2,4,5,3), C=(1,2,5,3,4), D=(1,3,5,4,2), E=(1,3,2,5,4), F=(1,3,4,2,5), G=(1,5,4,3,2), H=(1,5,3,2,4), I=(1,5,2,4,3), J=(1,4,2,3,5), K=(1,4,5,2,3), L=(1,4,3,5,2)

We'd like to view these elements as the vertices of a truncated tetrahedron, so we need to find the 4 triangles and the 6 connecting edges between them. The first task calls for order 3 elements, the second one for order two elements.



Take a conjugacy class of order 3 elements in A_4 say $T = (2,4,3),(1,2,3),(1,3,4),(1,4,2)$ and observe that when one computes the products of T with a fixed 5-cycle in the conjugacy class C there is a unique element among the four obtained that belongs to the conjugacy class C. This gives a cyclic action on C with orbits of length 3 (the triangles). Here they are :

$A \longrightarrow J \longrightarrow F \longrightarrow A$

$B \longrightarrow C \longrightarrow H \longrightarrow B$

$D \longrightarrow G \longrightarrow E \longrightarrow D$

$I \longrightarrow L \longrightarrow K \longrightarrow I$

For the edges, take the conjugacy class $S = (1,2)(3,4),(1,3)(2,4),(1,4)(2,3)$ of order two elements in A_4 and compute for any 5-cycle c in C the products and observe that among the elements obtained there is again one element belonging to C. This gives the following pairing

$A \leftrightarrow C, B \leftrightarrow I, D \leftrightarrow F, E \leftrightarrow H, G \leftrightarrow L$ and $J \leftrightarrow K$

and a bit of puzzling shows that all this can indeed be realized within a truncated tetrahedron (on the right). As to her other request

" and how about a post on how $1+4+9+ \ +24^2 = 70^2$ is REALLY a statement about unifying cusps and holes (genus) as degrees of freedom in quantum geometry?"

The scarecrow will need to take some time to think before giving his answer...

1.19 Tetra lattices

Error-correcting codes can be used to construct interesting lattices, the best known example being the Leech lattice constructed from the binary Golay code. Recall that a *lattice* L in $\mathbb{R}^n$ is the set of all integral linear combinations of n linearly independent vectors $\{v_1,\ldots,v_n\}$, that is

$L = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$

The theta function of the lattice is the power series

$\Theta_L(q) = \sum_l a_l q^l$

with a_l being the number of vectors in L of squared length l. If all squared lengths are even integers, the lattice is called *even* and if it has one point per unit volume, we call it *unimodular*. The theta function of an even unimodular lattice is a modular form. One of the many gems from Conway's book The sensual (quadratic) form is the chapter "Can You Hear the Shape of a Lattice?" or in other words, whether the theta function determines the lattice.

Ernst Witt knew already that there are just two even unimodular lattices in 16 dimensions : $E_* \oplus E_8$ and D_{16}^+ and as there is just one modular form of weigth 8 upto scalars, the theta function cannot determine the latice in 16 dimensions. The number of dimensions for a counterexample was subsequently reduced to 12 (Kneser), 8 (Kitaoka),6 (Sloane) and finally 4 (Schiemann).

Fig. 1.6: Ernst Witt

Sloane and Conway found an elegant counterexample in dimension 4 using two old friends : *the tetracode* and the *taxicab number* $1729 = 7x13x19$.

Recall that the *tetra code* is a one-error correcting code consisting of the following nine words of length four over $\mathbb{F}_3 = \{0, +, -\}$

$$\begin{array}{lll} 0\,000 & 0\,{+}{+}{+} & 0\,{-}{-}{-} \\ {+}\,0\,{+}\,{-} & {+}\,{+}\,{-}0 & {+}\,{-}\,0{+} \\ {-}\,0\,{-}\,{+} & {-}\,{+}\,0{-} & {-}\,{-}\,{+}0 \end{array}$$

The first element (which is slightly offset from the rest) is the *slope* s of the words, and the other three digits cyclically increase by s (in the field $\mathbb{F}_3$). Now take four mutually orthogonal vectors in $\mathbb{R}^4$ with square lengths

$$e_a.e_a = \tfrac{1}{12}, e_b.e_b = \tfrac{7}{12}, e_c.e_c = \tfrac{13}{12}, e_d.e_d = \tfrac{19}{12}$$

and denote with (w, x, y, z) the vector $we_a + xe_b + ye_c + ze_d$. Now consider the two lattices L^+ respectively L^- spanned by the vectors $(3, -1, -1, -1), (1, 3, 1, -1), (1, -1, 3, 1)$ $(1, 1, -1, 3), (-3, -1, -1, -1), (1, -3, 1, -1)$ $(1, -1, -3, 1), (1, 1, -1, -3)$

then it follows that if we reduce any vector in either lattice modulo 3 we get a tetracode word. Using this fact it is not too difficult to show that there is a *length preserving* bijection between L^+ and L^- given by the rule : *change the sign of the first coordinate that is divisible by 3*. As a direct consequence, the theta functions of these two lattices are equal.

Yet, these lattices cannot be isometric. One verifies that the only vectors of norm 4 in L^+ are $\pm(3, -1, -1, -1)$ and those of norm 8 are $\pm(1, 3, 1, -1)$ and one computes that their in-product is

$$(3, -1, -1, -1).(1, 3, 1, -1) = -1$$

Similarly, the only vectors of norm 4 in L^- are $\pm(-3, -1, -1, -1)$ and those of norm 8 are $\pm(1, -3, 1, -1)$ whereas their in-product is

$$(-3, -1, -1, -1).(1, -3, 1, -1) = 2$$

so the two lattices are different!

Reference : John H. Conway, "The sensual (quadratic) form" second lecture "Can you hear the shape of a lattice?"

1.20 Who discovered the Leech lattice (1/2)

The Leech lattice was, according to wikipedia, 'originally discovered by Ernst Witt in 1940, but he did not publish his discovery' and it 'was later re-discovered in 1965 by John Leech'. However, there is very little evidence to support this claim.

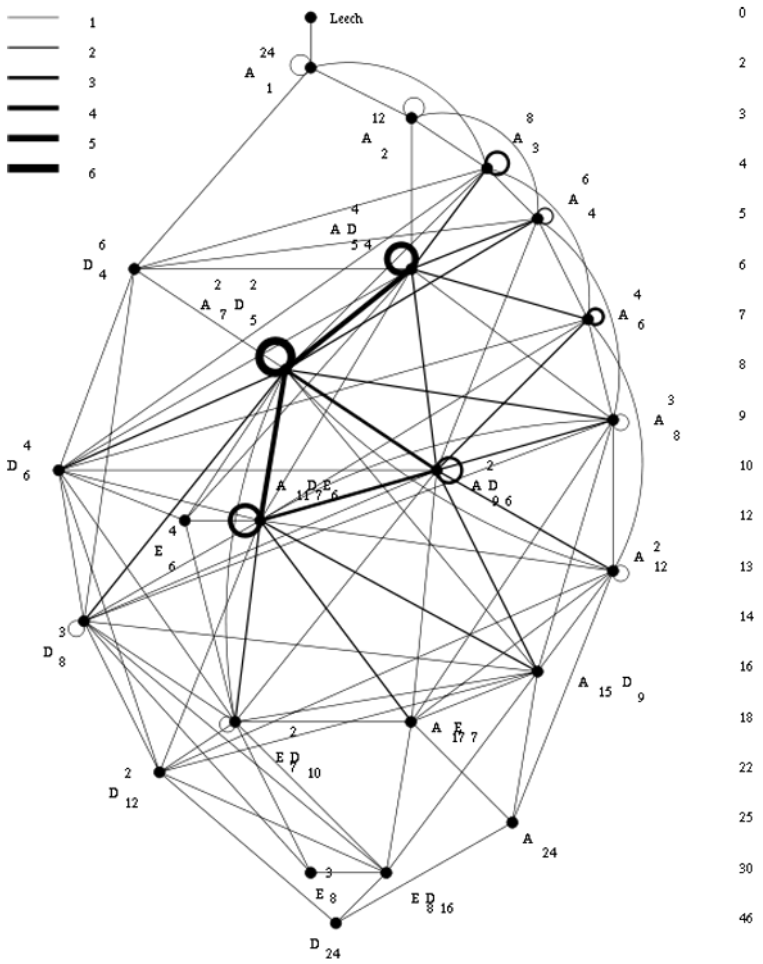
The facts

What is certain is that John Leech discovered in 1965 an amazingly dense 24-dimensional lattice Λ having the property that unit balls around the lattice points touch, each one of them having exactly 196560 neighbors. The paper 'Notes on sphere packings' appeared in 1967 in the Canad. J. Math. 19, 251-267.

Compare this to the optimal method to place pennies on a table, leading to the hexagonal tiling, each penny touching exactly 6 others. Similarly, in dimension 8 the densest packing is the E8 lattice in which every unit ball has exactly 240 neighbors.

The Leech lattice Λ can be characterized as the unique unimodular positive definite even lattice such that the length of any non-zero vector is at least two.

The list of all positive definite even unimodular lattices, Γ_{24}, in dimension 24 was classified later by Hans-Volker Niemeier and are now known as the 24 Niemeier lattices.



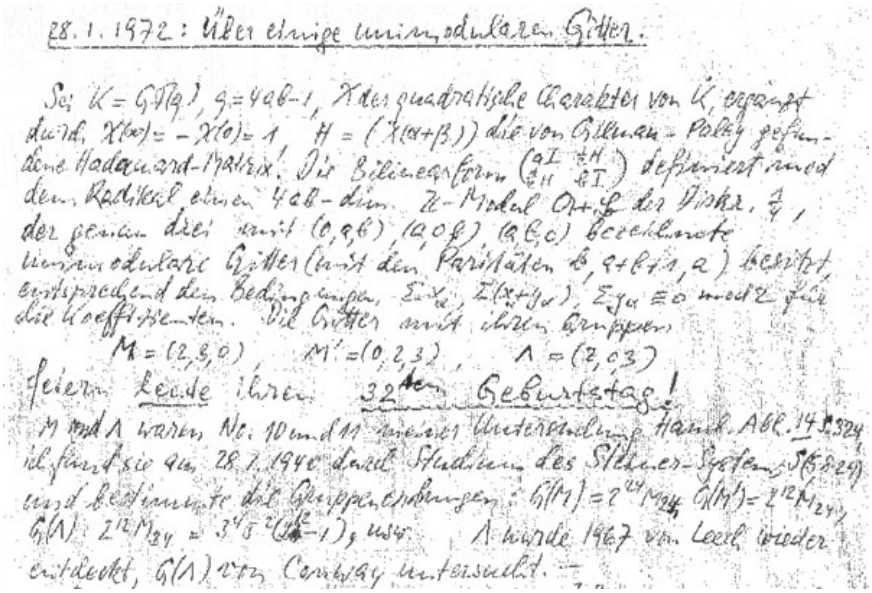
For the chronology below it is perhaps useful to note that, whereas Niemeier's paper did appear in 1973, it was submitted april 5th 1971 and is just a minor rewrite of Niemeier's Ph.D. "Definite quadratische Formen der Dimension 24 und Diskriminante 1" obtained in 1968 from the University of Gttingen with advisor Martin Kneser.

The claim

On page 328 of Ernst Witt's Collected Papers Ina Kersten recalls that Witt gave a colloquium talk on January 27, 1970 in Hamburg entitled "Gitter und Mathieu-Gruppen" (Lattices and Mathieu-groups).

In this talk Witt claimed to have found nine lattices in Γ_{24} as far back as 1938 and that on January 28, 1940 he found two additional lattices M and Λ while studying the Steiner system $S(5,8,24)$.

On page 329 of the collected papers is a scan of the abstract Witt wrote in the colloquium book in Bielefeld where he gave a talk "Uber einige unimodularen Gitter" (On certain unimodular lattices) on January 28, 1972


28. 1. 1972: Über einige unimodularen Gitter.

Sei $K = GF(q)$, $q = 4a^2b - 1$, χ der quadratische Charakter von K, ergänzt durch $\chi(0) = -\chi(0) = 1$, $H = (\chi(\alpha+\beta))$ die von Gilman-Paley gefundene Hadamard-Matrix. Die Bilinearform $\begin{pmatrix} aI & +H \\ +H & bI \end{pmatrix}$ definiert modd den Radikal einen $4ab$-dim. $\mathfrak{k}$-Modul O^+ der Diskr. $\frac{1}{q}$, der genau drei mit (a,q,b), (a,a,β), (α,β,a) beschriebene unimodulare Gitter (mit den Parametern $b, q+b+1, a$) beherbergt, entsprechend den Bedingungen Σx_α, $\Sigma(x+y_\alpha)$, $\Sigma y_\alpha \equiv 0 \bmod 2$ für die Koeffizienten. Die Gitter mit ihren Gruppen

$M = (2,3,0)$, $M' = (0,2,3)$, $\Lambda = (2,0,3)$

feiern heute ihren 32ten Geburtstag!

M und Λ waren Nr. 10 und 11 meiner Untersuchung Hamb. Abh. 14 S. 324 ff. sie fand am 28. 1. 1940 beim Studium des Steiner-Systems $S(5,8,24)$ und bestimmte die Gruppenordnungen: $G(M) = 2^{14} M_{24}$, $G(M') = 2^{12} M_{24}$, $G(\Lambda) = 2^{12} M_{24} \cdot 3^4 5^2 (7^2 - 1)$, usw. Λ wurde 1967 von Leech wieder entdeckt, $G(\Lambda)$ von Conway untersucht. –

Here, Witt claims that he found three new lattices in Γ_{24} on January 28, 1940 as the lattices M, M' and Λ 'feiern heute ihren 32sten Geburstag!' (celebrate today their 32nd birthday).

He goes on telling that the lattices M and Λ were number 10 and 11 in his list of lattices in Γ_{24} in his paper "Eine Identität zwischen Modulformen zweiten Grades" in the Abh. Math. Sem. Univ. Hamburg 14 (1941) 323-337 and he refers in particular to page 324 of that paper.

He further claims that he computed the orders of their automorphism groups and writes that Λ 'wurde 1967 von Leech wieder-entdeckt' (was re-discovered by Leech in 1967) and that its automorphism group $G(\Lambda)$ was studied by John Conway. Recall that Conway's investigations of the automorphism group of the Leech lattice led to the discovery of three new sporadic groups, the Conway groups Co_1, Co_2 and Co_3. However, Witt's 1941-paper does not contain a numbered list of 24-dimensional lattices. In fact, apart from $E_8 + E_8 + E_8$ is does not contain a single lattice in Γ_{24}. The only relevant paragraph is indeed on page 324

324 E. Witt.

Summen $\Theta_8 + \Theta_8 + \cdots$ ergibt sich hieraus die Existenz von Γ_m für jedes $m \equiv 0 \bmod 8$. Übrigens ist für die Existenz von Γ_m die Bedingung $8 \mid m$ auch notwendig, wie sich etwa aus der Reziprozitätsformel für Gaußsche Summen ergibt. Nach MORDELL ist $h_8 = 1$. Ich werde hier beweisen, daß $h_{16} = 2$ ist. Dabei werde ich die beiden Klassen explizit angeben. SCHOENEBERG bewies kürzlich in einer Arbeit über Modulformen, daß es außer $\Theta_8 + \Theta_8 + \Theta_8$ noch eine weitere Klasse in Γ_{24} geben muß. Bei dem Versuch, eine Form aus einer solchen Klasse wirklich anzugeben, fand ich mehr als 10 verschiedene Klassen in Γ_{24}. Die Bestimmung von h_{24} scheint nicht ganz leicht zu sein.

He observes that Mordell already proved that there is just one lattice in Γ_8 (the E_8-lattice) and that the main result of his paper is to prove that there are precisely two even unimodular 16-dimensional lattices : $E_8 + E_8$ and another lattice, now usually called the 16-dimensional Witt-lattice.

He then goes on to observe that Schoeneberg knew that $\#\Gamma_{24} > 1$ and so there must be more lattices than $E_8 + E_8 + E_8$ in Γ_{24}. Witt concludes with : "In my attempt to find such a lattice, I discovered more than 10 lattices in Γ_{24}. The determination of $\#\Gamma_{24}$ does not seem to be entirely trivial."

Hence, it is fair to assume that by 1940 Ernst Witt had discovered at least 11 of the 24 Niemeier lattices. Whether the Leech lattice was indeed lattice 11 on the list is anybody's guess.

Next time we will look more closely into the historical context of Witt's 1941 paper.

1.21 Who discovered the Leech lattice (2/2)

For the better part of the 30ties, Ernst Witt (1) did hang out with the rest of the 'Noetherknaben', the group of young mathematicians around Emmy Noether (3) in Gottingen.

In 1934 Witt became Helmut Hasse's assistent in Gottingen, where he qualified as a university lecturer in 1936. By 1938 he has made enough of a name for himself to be offered a lecturer position in Hamburg and soon became an associate professor, the down-graded position held by Emil Artin (2) until he was forced to emigrate in 1937.

A former fellow student of him in Gottingen, Erna Bannow (4), had gone earlier to Hamburg to work with Artin. She continued her studies with Witt and finished her Ph.D. in 1939. In 1940 Erna Bannow and Witt married.

So, life was smiling on Ernst Witt that sunday january 28th 1940, both professionally and personally. There was just one cloud on the horizon, and a rather menacing one. He was called up by the Wehrmacht and knew he had to enter service in february. For all he knew,

he was spending the last week-end with his future wife... (later in february 1940, Blaschke helped him to defer his military service by one year). Still, he desperately wanted to finish his paper before entering the army, so he spend most of that week-end going through the final version and submitted it on monday, as the published paper shows.

Eine Identität zwischen Modulformen zweiten Grades. 337

führung des Satzes ergibt. Einen trivialen euklidischen Algorithmus gibt es nun in jedem Körper. *Satz C gilt demnach auch, wenn etwa von reellen statt von ganzzahligen Matrizen die Rede ist.* Auf Grund dieser Bemerkung läßt sich beweisen, daß

$$(41) \qquad |\mathfrak{Y}|^{-n-1} \prod_{\alpha \leq \beta} (dx_{\alpha\beta}\, dy_{\alpha\beta}) \qquad (\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y})$$

ein alternierender Differentialausdruck ist, der bei allen reellen Modulsubstitutionen (40) invariant bleibt. Der Beweis soll aber hier unterdrückt werden, da es einen anderen, direkten und von Satz C unabhängigen Beweis für die behauptete Invarianz gibt und weil von dieser Invarianz in der vorliegenden Arbeit doch nirgends Gebrauch gemacht wird.

Hamburg, den 29. Januar 1940.

In the 70ties, Witt suddenly claimed he did discover the Leech lattice Λ that sunday. In the last section we have seen that the only written evidence for Witt's claim is one sentence in his 1941-paper Eine Identität zwischen Modulformen zweiten Grades. "Bei dem Versuch, eine Form aus einer solchen Klassen wirklich anzugeben, fand ich mehr als 10 verschiedene Klassen in Γ_{24}."

But then, why didn't Witt include more details of this sensational lattice in his paper?

Ina Kersten recalls on page 328 of Witt's collected papers : "In his colloquium talk "Gitter und Mathieu-Gruppen" in Hamburg on January 27, 1970, Witt said that in 1938, he had found nine lattices in Γ_{24} and that later on January 28, 1940, while studying the Steiner system $S(5, 8, 24)$, he had found two additional lattices M and Λ in Γ_{24}. He continued saying that he had then given up the tedious investigation of Γ_{24} because of the surprisingly low contribution

$$|Aut(\Lambda)|^{-1} < 10^{-18}$$

to the Minkowski density and that he had consented himself with a short note on page 324 in his 1941 paper."

In the last sentence he refers to the fact that the sum of the inverse orders of the automorphism groups of all even unimodular lattices of a given dimension is a fixed rational number, the Minkowski-Siegel mass constant. In dimension 24 this constant is

$$\sum_L \frac{1}{|Aut(L)|} = \frac{1027637932586061520960267}{129477933340026851560636148613120000000} \approx 7.937 \times 10^{-15}$$

That is, Witt was disappointed by the low contribution of the Leech lattice to the total constant and concluded that there might be thousands of new even 24-dimensional unimodular lattices out there, and dropped the problem.

If true, the story gets even better : not only claims Witt to have found the lattices $A_1^{24} = M$ and Λ, but also enough information on the Leech lattice in order to compute the order of its automorphism group $Aut(\Lambda)$, aka the Conway group $Co_0 = .0$ the dotto-group!

Is this possible? Well fortunately, the difficulties one encounters when trying to compute the order of the automorphism group of the Leech lattice from scratch, is one of the better documented mathematical stories around.

The books From Error-Correcting Codes through Sphere Packings to Simple Groups by Thomas Thompson, Symmetry and the monster by Mark Ronan, and Finding moonshine by Marcus du Sautoy tell the story in minute detail.

It took John Conway 12 hours on a 1968 saturday in Cambridge to compute the order of the dotto group, using the knowledge of Leech and McKay on the properties of the Leech lattice and with considerable help offered by John Thompson via telephone.

But then, John Conway is one of the fastest mathematicians the world has known. The prologue of his book On numbers and games begins with : "Just over a quarter of a century ago, for seven consecutive days I sat down and typed from 8:30 am until midnight, with just an hour for lunch, and ever since have described this book as "having been written in a week"."

Conway may have written a book in one week, Ernst Witt did complete his entire Ph.D. in just one week! In a letter of August 1933, his sister told her parents : "He did not have a thesis topic until July 1, and the thesis was to be submitted by July 7. He did not want to have a topic assigned to him, and when he finally had the idea, he started working day and night, and eventually managed to finish in time."

So, if someone might have beaten John Conway in fast-computing the dottos order, it may very well have been Witt. Sadly enough, there is a lot of circumstantial evidence to make Witt's claim highly unlikely.

For starters, psychology. Would you spend your last week-end together with your wife to be before going to war performing an horrendous calculation?

Secondly, mathematical breakthroughs often arise from newly found insight. At that time, Witt was also working on his paper on root lattices "Spiegelungsgrupen and Aufzähling halbeinfacher Liescher Ringe" which he eventually submitted in january 1941. Contained in that paper is what we know as Witt's lemma which tells us that for any integral lattice the sublattice generated by vectors of norms 1 and 2 is a direct sum of root lattices.

This leads to the trick of trying to construct unimodular lattices by starting with a direct sum of root lattices and 'adding glue'. Although this gluing-method was introduced by Kneser as late as 1967, Witt must have been aware of it as his 16-dimensional lattice D_{16}^+ is constructed this way.

If Witt wanted to construct new 24-dimensional even unimodular lattices in 1940, it would be natural for him to start off with direct sums of root lattices and trying to add vectors to them until he got what he was after. Now, all of the Niemeier-lattices are constructed this way, except for the Leech lattice!

Lattice	Glue (omitting commas)
$(D_{24})^+$	[1]
$(D_{16}E_8)^+$	[10]
E_8^3	[000]
$(A_{24})^+$	[5]
$(D_12^2)^+$	[12, 21]
$(A_{17}E_7)^+$	[31]
$(D_{10}E_7^2)^+$	[110, 301]
$(A_{15}D_9)^+$	[21]
$(D_8^3)^+$	[(122)]
$(A_{12}^2)^+$	[15]
$(A_{11}D_7E_6)^+$	[11]
$(E_6^4)^+$	[1(012)]
$(A_9^2D_6)^+$	[240, 501, 053]
$(D_6^4)^+$	[even perms of (0123)]
$(A_8^3)^+$	[(114)]
$(A_7^2D_5^2)^+$	[1112, 1721]
$(A_6^4)^+$	[1(216)]
$(A_5^4D_4)^+$	[(2(024)0, 33001, 30302, 30033]
$(D_4^6)^+$	[111111, 0(02332)]
$(A_4^6)^+$	[1(01441)]
$(A_3^8)^+$	[3(2001011)]
$(A_2^{12})^+$	[2(11211122212)]
$(A_1^{24})^+$	[1(000001010011001101011111)]
Λ_{24}	(not obtainable by this method)

I'm far from an expert on the Niemeier lattices but I would say that Witt definitely knew of the existence of D_{24}^+, E_8^3 and A_{24}^+ and that it is quite likely he also constructed $(D_{16}E_8)^+, (D_{12}^2)^+, (A_{12}^2)^+, (D_8^3)^+$ and possibly $(A_{17}E_7)^+$ and $(A_{15}D_9)^+$. I'd rate it far more likely Witt constructed another two such lattices on sunday january 28th 1940, rather than discovering the Leech lattice.

Finally, wouldn't it be natural for him to include a remark, in his 1941 paper on root lattices, that not every even unimodular lattices can be obtained from sums of root lattices by adding glue, the Leech lattice being the minimal counter-example?

If it is true he was playing around with the Steiner systems that sunday, it would still be a pretty good story he discovered the lattices $(A_2^{12})^+$ and $(A_1^{24})^+$, for this would mean he discovered the Golay codes in the process!

Which brings us to our next question : who discovered the Golay code?

1.22 Sporadic simple games

Above I did a series of posts on games associated to the Mathieu sporadic group M_{12}, starting with the section on *Conway's puzzle* M_{13}, and, continuing with a discussion of *mathematical blackjack*. The idea at the time was to write a book for a general audience, ending with a series of new challenging mathematical games. I asked : "What kind of puzzles should we promote for mathematical thinking to have a fighting chance to survive in the near future?"

Now, Scientific American has (no doubt independently) taken up this lead. Their July 2008 issue features the article Rubik's Cube Inspired Puzzles Demonstrate Math's "Simple Groups" written by Igor Kriz and Paul Siegel.

By far the nicest thing about this article is that it comes with three online games based on the sporadic simple groups, the Mathieu groups M_{12}, M_{24} and the Conway group .0.

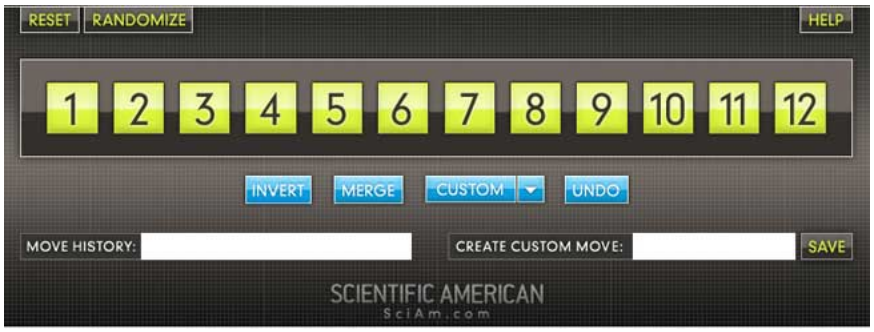
the M_{12} game

Scrambles to an arbitrary permutation in M_{12} and need to use the two generators

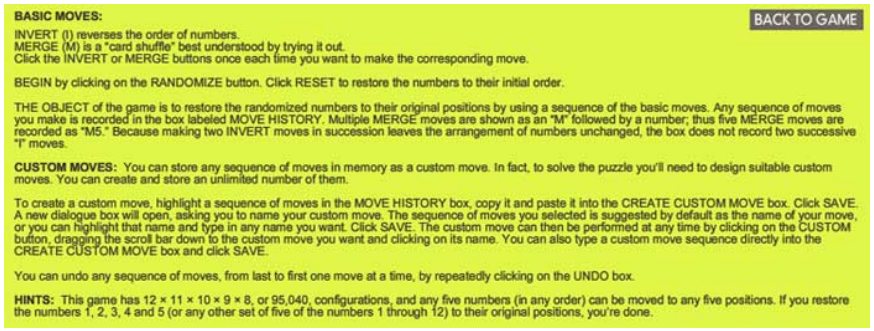
$INVERT = (1,12)(2,11)(3,10)(4,9)(5,8)(6,7)$ and

$MERGE = (2,12,7,4,11,6,10,8,9,5,3)$

to return to starting position.



Here is the help-screen :



A few-line GAP-program cracks the puzzle instantly.

the M_{24} game

Similar in nature, again using two generators of M_{24}. GAP-solution as before.

This time, they offer this help-screen :

BASIC MOVES:
LEFT (L) and RIGHT (R) shift all the numbers except the topmost number by one "notch" around the big circle (LEFT is counterclockwise; RIGHT is clockwise). You can shift any number of notches left or right by clicking and dragging your mouse inside the big circle of numbers.
SWITCH (S) exchanges every pair of numbers with the same color. Click the SWITCH button in the middle to make the move.

BEGIN by clicking on the RANDOMIZE button.

Click RESET to restore the numbers to their initial positions.

THE OBJECT of the game, as with the M12 game, is to restore the randomized numbers to their original positions by using a sequence of the basic moves. Any sequence of moves you make is recorded in the box labeled MOVE HISTORY. Multiple LEFT or RIGHT moves are shown as an "L" or an "R" followed by a number; thus dragging five notches to the left (rotating the numbers counterclockwise) is recorded as "L5." Because making two SWITCH moves in succession leaves the configuration unchanged, the box does not record two successive "S" moves.

CUSTOM MOVES:
Again as with the M12 game, you can store any sequence of moves in memory as a custom move. In fact, to solve the puzzle you'll need to design suitable custom moves. You can create and store an unlimited number of them.

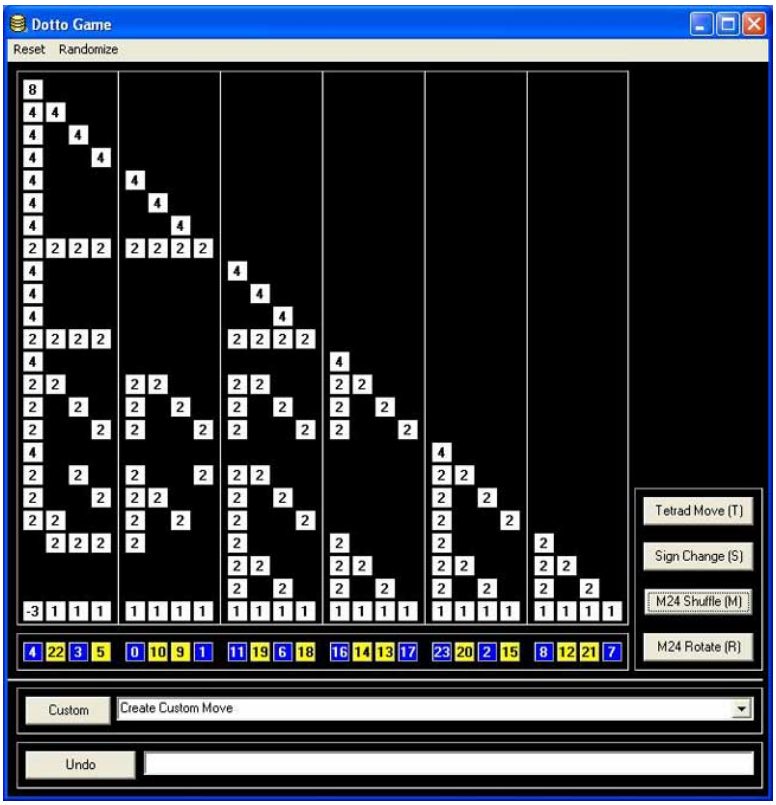
To create a custom move, highlight a sequence of moves in the MOVE HISTORY box, copy it and paste it into the CREATE CUSTOM MOVE box. Click SAVE. A new dialogue box will open, asking you to name your custom move. The sequence of moves you selected is suggested by default as the name of your move, or you can highlight that name and type in any name you want. Click SAVE. The custom move can then be performed at any time by clicking on the CUSTOM button, dragging the scroll bar down to the custom move you want and clicking on its name. You can also type a custom move sequence directly into the CREATE CUSTOM MOVE box and click SAVE.

You can undo any sequence of moves, from last to first one move at a time, by repeatedly clicking on the UNDO box.

HINTS:
This game has 24 × 23 × 22 × 21 × 20 × 48, or 244,823,040, configurations. As with the M12 puzzle, any five numbers (in any order) can be moved to any five positions. Once you restore the numbers 1, 2, 3, 4 and 5 (or any other set of five of the numbers 0 through 23) to their original positions, you're almost—but not quite—done. Because of the multiplier 48 among the factors above, once you get five numbers in position, you have reached one of 48 possible configurations. To solve the puzzle, you'll still have to devise moves that shift the remaining 19 numbers back to their original positions.

the .0 game

Their most original game is based on Conway's .0 (dotto) group. Unfortunately, they offer only a Windows-executable version, so I had to install Bootcamp and struggle a bit with taking screenshots on a MacBook to show you the game's starting position :



”Dotto:

Dotto, our final puzzle, represents the Conway group Co0, published in 1968 by mathematician John H. Conway of Princeton University. Co0 contains the sporadic simple group Co1 and has exactly twice as many members as Co1. Conway is too modest to name Co0 after himself, so he denotes the group .0 (hence the pronunciation dotto).

In Dotto, there are four moves. This puzzle includes the M24 puzzle. Look at the yellow/blue row in the bottom. This is, in fact, M24, but the numbers are arranged in a row instead of a circle. The R move is the ”circle rotation to the right”: the column above the number 0 stays put, but the column above the number 1 moves to the column over the number 2 etc. up to the column over the number 23, which moves to the column over the number 1. You may also click on a column number and then on another column number in the bottom row, and the ”circle rotation” moving the first column to the second occurs. The M move is the switch, in each group of 4 columns separated by vertical lines (called tetrads) the ”yellow” columns switch and the ”blue” columns switch. The sign change move (S) changes signs of the first 8 columns (first two tetrads). The tetrad move (T) is the most complicated: Subtract in each row from each tetrad 1/2 times the sum of the numbers in that tetrad. Then in addition to that, reverse the signs of the columns in the first tetrad.

Strategy hints: Notice that the sum of squares of the numbers in each row doesn’t change. (This sum of squares is 64 in the first row, 32 in every other row.) If you manage to get an ”8”in the first row, you have almost reduced the game to M24 except those signs. To have the original position, signs of all numbers on the diagonal must be +. Hint on signs: if the only thing wrong are signs on the diagonal, and only 8 signs are wrong, those 8 columns can be moved to the first 8 columns by using only the M24 moves (M,R).”

1.23 Monstrous frustrations

Thanks for clicking through to this section... I guess.

If nothing else, it shows that just as much as the stock market is fueled by greed, mathematical research is driven by frustration (or the pleasure gained from knowing others to be frustrated).

I did spend the better part of the day doing a lengthy, if not laborious, calculation, I've been postponing for several years now. Partly, because I didn't know how to start performing it (though the basic strategy was clear), partly, because I knew beforehand the final answer would probably offer me no further insight.

Still, it gives the final answer to a problem that may be of interest to anyone vaguely interested in Moonshine :

What does the Monster see of the modular group?

I know at least two of you, occasionally reading this blog, understand what I was trying to do and may now wonder how to repeat the straightforward calculation. Well the simple answer is : Google for the number 97239461142009186000 and, no doubt, you will be able to do the computation overnight.

One word of advice : *don't!* Get some sleep instead, or make love to your partner, because all you'll get is a quiver on nine vertices (which is pretty good for the Monster) but having an horrible amount of loops and arrows...

If someone wants the details on all of this, just ask. But, if you really want to get me exited : find a moonshine reason for one of the following two numbers :

$$7916163813959324092654301441657645004 92 =$$

$$2^2 * 11 * 293 * 614036907691539256333718696994853 01$$

(the dimension of the monster-singularity up to smooth equivalence), or,

$$1575918800531316887592467826675348205163 =$$

$$523 * 1655089391 * 15982020053213 * 113914503502907$$

(the dimension of the moduli space).

1.24 What does the monster see?

The Monster is the largest of the 26 sporadic simple groups and has order

$$808.017.424.794.512.875.886.459.904.961.710.757.005.754.368.000.000.000 =$$

$$2^{46}3^{20}5^9 7^6 11^2 13^3 17.19.23.29.31.41.47.59.71$$

It is not so much the size of its order that makes it hard to do actual calculations in the monster, but rather the dimensions of its smallest non-trivial irreducible representations (196.883 for the smallest, 21.296.876 for the next one, and so on).

In characteristic two there is an irreducible representation of one dimension less (196882) which appears to be of great use to obtain information. For example, Robert Wilson used it to prove that The Monster is a Hurwitz group. This means that the Monster is generated by two elements g and h satisfying the relations

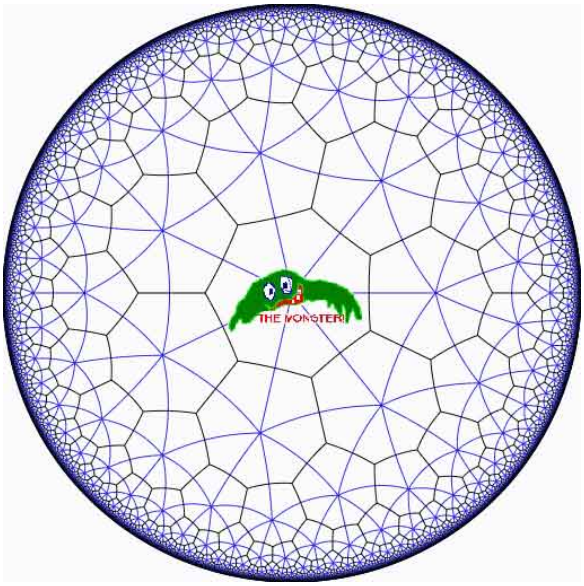
$$g^2 = h^3 = (gh)^7 = 1$$

Geometrically, this implies that the Monster is the automorphism group of a Riemann surface of genus gen satisfying the Hurwitz bound $84(gen-1) = \#\text{Monster}$. That is,

$gen = 96192550570775342367435702971632232976875520000000001 =$

$42151199 * 293998543 * 7762226826038285371428139684528301 93$

Or, in analogy with the *Klein quartic* (see the buckyball curve section) which can be constructed from 24 heptagons in the tiling of the hyperbolic plane, there is a finite region of the hyperbolic plane, tiled with heptagons, from which we can construct this monster curve by gluing the boundary is a specific way so that we get a Riemann surface with exactly $96192550570775342367435702971632232976875520000000001$ holes. This finite part of the hyperbolic tiling (consisting of $\#\text{Monster}/7$ heptagons) we'll call the *empire of the monster* and we'd love to describe it in more detail.



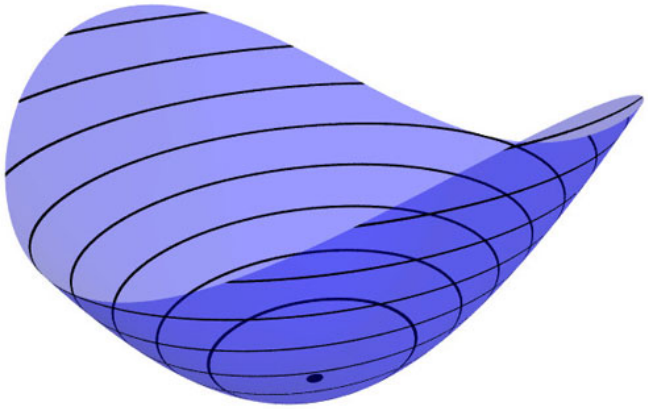
Look at the half-edges of all the heptagons in the empire (the picture above learns that every edge in cut in two by a blue geodesic). They are exactly $\#\text{Monster}$ such half-edges and they form a *dessin d'enfant* for the monster-curve.

If we label these half-edges by the elements of the Monster, then multiplication by g in the monster interchanges the two half-edges making up a heptagonal edge in the empire and multiplication by h in the monster takes a half-edge to the one encountered first by going counter-clockwise in the vertex of the heptagonal tiling. Because g and h generated the Monster, the dessin of the empire is just a concrete realization of the monster.

Because g is of order two and h is of order three, the two permutations they determine on the dessin, gives a group epimorphism $C_2 * C_3 = PSL_2(\mathbb{Z}) \to \mathbb{M}$ from the modular group $PSL_2(\mathbb{Z})$ onto the Monster-group.

In noncommutative geometry, the group-algebra of the modular group $\mathbb{C}PSL_2$ can be interpreted as the coordinate ring of a noncommutative manifold (because it is formally smooth in the sense of Kontsevich-Rosenberg or Cuntz-Quillen) and the group-algebra of the Monster $\mathbb{CM}$ itself corresponds in this picture to a finite collection of 'points' on the manifold. Using this geometric viewpoint we can now ask the question *What does the Monster see of the modular group?*

To make sense of this question, let us first consider the commutative equivalent : what does a point P see of a commutative variety X?



Evaluation of polynomial functions in P gives us an algebra epimorphism $\mathbb{C}[X] \to \mathbb{C}$ from the coordinate ring of the variety $\mathbb{C}[X]$ onto $\mathbb{C}$ and the kernel of this map is the maximal ideal $\mathfrak{m}_P$ of $\mathbb{C}[X]$ consisting of all functions vanishing in P.

Equivalently, we can view the point $P = \mathbf{spec}\ \mathbb{C}[X]/\mathfrak{m}_P$ as the scheme corresponding to the quotient $\mathbb{C}[X]/\mathfrak{m}_P$. Call this the 0-th formal neighborhood of the point P.

This sounds pretty useless, but let us now consider higher-order formal neighborhoods. Call the affine scheme $\mathbf{spec}\ \mathbb{C}[X]/\mathfrak{m}_P^{n+1}$ the n-th forml neighborhood of P, then the first neighborhood, that is with coordinate ring $\mathbb{C}[X]/\mathfrak{m}_P^2$ gives us tangent-information. Alternatively, it gives the best linear approximation of functions near P. The second neighborhood $\mathbb{C}[X]/\mathfrak{m}_P^3$ gives us the best quadratic approximation of function near P, etc. etc.

These successive quotients by powers of the maximal ideal $\mathfrak{m}_P$ form a system of algebra epimorphisms

$$\ldots \frac{\mathbb{C}[X]}{\mathfrak{m}_P^{n+1}} \to \frac{\mathbb{C}[X]}{\mathfrak{m}_P^{n}} \to \ldots\ldots \to \frac{\mathbb{C}[X]}{\mathfrak{m}_P^{2}} \to \frac{\mathbb{C}[X]}{\mathfrak{m}_P} = \mathbb{C}$$

and its inverse limit $\underset{\leftarrow}{lim}\ \frac{\mathbb{C}[X]}{\mathfrak{m}_P^n} = \hat{\mathcal{O}}_{X,P}$ is the completion of the local ring in P and contains all the infinitesimal information (to any order) of the variety X in a neighborhood of P. That is, this completion $\hat{\mathcal{O}}_{X,P}$ contains *all information that P can see of the variety X*.

In case P is a smooth point of X, then X is a manifold in a neighborhood of P and then this completion $\hat{\mathcal{O}}_{X,P}$ is isomorphic to the algebra of formal power series $\mathbb{C}[[x_1, x_2, \ldots, x_d]]$ where the x_i form a local system of coordinates for the manifold X near P.

Right, after this lengthy recollection, back to our question *what does the monster see of the modular group?* Well, we have an algebra epimorphism

$$\pi\ :\ \mathbb{C}PSL_2(\mathbb{Z}) \to \mathbb{CM}$$

and in analogy with the commutative case, all information the Monster can gain from the modular group is contained in the $\mathfrak{m}$-adic completion

$$\widehat{\mathbb{C}PSL_2(\mathbb{Z})}_{\mathfrak{m}} = \underset{\leftarrow}{lim}\ \frac{\mathbb{C}PSL_2(\mathbb{Z})}{\mathfrak{m}^n}$$

where $\mathfrak{m}$ is the kernel of the epimorphism π sending the two free generators of the modular group $PSL_2(\mathbb{Z}) = C_2 * C_3$ to the permutations g and h determined by the dessin of the pentagonal tiling of the Monster's empire.

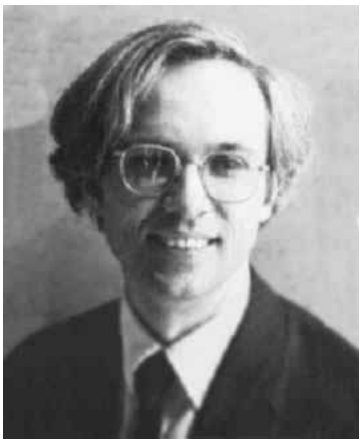
As it is a hopeless task to determine the Monster-empire explicitly, it seems even more hopeless to determine the kernel $\mathfrak{m}$ let alone the completed algebra... But, (surprise) we can compute $\widehat{\mathbb{C}PSL_2(\mathbb{Z})}_{\mathfrak{m}}$ as explicitly as in the commutative case we have $\hat{\mathcal{O}}_{X,P} \simeq \mathbb{C}[[x_1, x_2, \ldots, x_d]]$ for a point P on a manifold X.

Here the details : the quotient $\mathfrak{m}/\mathfrak{m}^2$ has a natural structure of $\mathbb{CM}$-bimodule. The group-algebra of the monster is a semi-simple algebra, that is, a direct sum of full matrix-algebras of sizes corresponding to the dimensions of the irreducible monster-representations. That is,

$$\mathbb{CM} \simeq \mathbb{C} \oplus M_{196883}(\mathbb{C}) \oplus M_{21296876}(\mathbb{C}) \oplus \ldots\ldots \oplus M_{258823477531055064045234375}(\mathbb{C})$$

with exactly 194 components (the number of irreducible Monster-representations). For any $\mathbb{CM}$-bimodule M one can form the tensor-algebra

$$T_{\mathbb{CM}}(M) = \mathbb{CM} \oplus M \oplus (M \otimes_{\mathbb{CM}} M) \oplus (M \otimes_{\mathbb{CM}} M \otimes_{\mathbb{CM}} M) \oplus \ldots\ldots$$

and applying the formal neighborhood theorem for formally smooth algebras (such as $\mathbb{C}PSL_2(\mathbb{Z})$) due to Joachim Cuntz (left) and Daniel Quillen (right) we have an isomorphism of algebras

$$\widehat{\mathbb{C}PSL_2(\mathbb{Z})}_{\mathfrak{m}} \simeq T_{\mathbb{CM}}\widehat{(\mathfrak{m}/\mathfrak{m}^2)}$$

where the right-hand side is the completion of the tensor-algebra (at the unique graded maximal ideal) of the $\mathbb{CM}$-bimodule $\mathfrak{m}/\mathfrak{m}^2$, so we'd better describe this bimodule explicitly.

Okay, so what's a bimodule over a semisimple algebra of the form $S = M_{n_1}(\mathbb{C}) \oplus \ldots \oplus M_{n_k}(\mathbb{C})$? Well, a *simple* S-bimodule must be either (1) a factor $M_{n_i}(\mathbb{C})$ with all other factors acting trivially or (2) the full space of rectangular matrices $M_{n_i \times n_j}(\mathbb{C})$ with the factor $M_{n_i}(\mathbb{C})$ acting on the left, $M_{n_j}(\mathbb{C})$ acting on the right and all other factors acting trivially.

That is, any S-bimodule can be represented by a quiver (that is a directed graph) on k vertices (the number of matrix components) with a loop in vertex i corresponding to each simple factor of type (1) and a directed arrow from i to j corresponding to every simple factor of type (2).

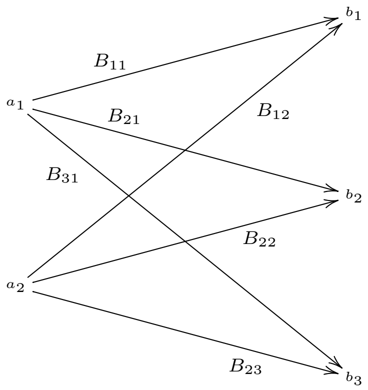
That is, for the Monster, the bimodule $\mathfrak{m}/\mathfrak{m}^2$ is represented by a quiver on 194 vertices and now we only have to determine how many loops and arrows there are at or between vertices.

Using Morita equivalences and standard representation theory of quivers it isn't exactly rocket science to determine that the number of arrows between the vertices corresponding to the irreducible Monster-representations S_i and S_j is equal to

$$dim_{\mathbb{C}}\ Ext^1_{\mathbb{C}PSL_2(\mathbb{Z})}(S_i, S_j) - \delta_{ij}$$

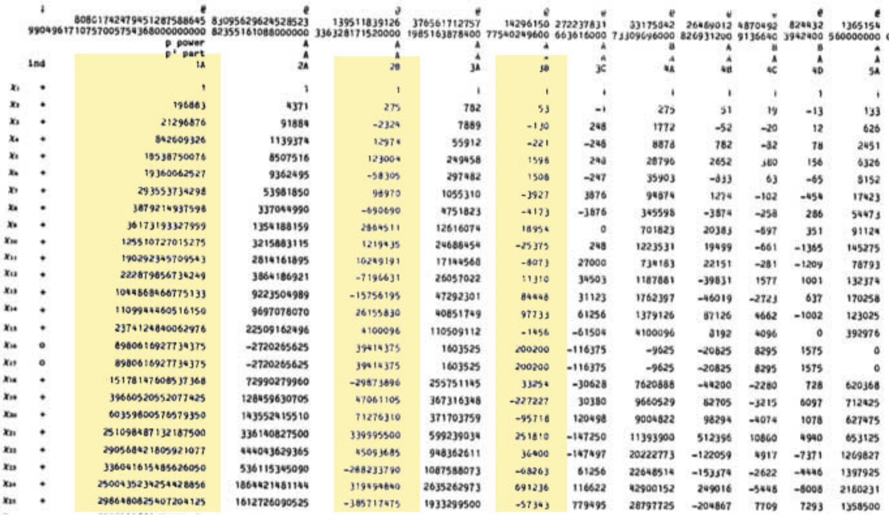
Now, I've been wasting a lot of time already explaining what representations of the modular group have to do with quivers and for quiver-representations we all know how to compute

Ext-dimensions in terms of the Euler-form applied to the dimension vectors. Right, so for every Monster-irreducible S_i we have to determine the corresponding dimension-vector $(a_1, a_2; b_1, b_2, b_3)$ for the quiver



Now the dimensions a_i are the dimensions of the ± 1 eigenspaces for the order 2 element g in the representation and the b_i are the dimensions of the eigenspaces for the order 3 element h. So, we have to determine to which conjugacy classes g and h belong, and from Wilson's paper mentioned above these are classes 2B and 3B in standard Atlas notation.

So, for each of the 194 irreducible Monster-representations we look up the character values at 2B and 3B (see below for the first batch of those) and these together with the dimensions determine the dimension vector $(a_1, a_2; b_1, b_2, b_3)$.



		@	@	@	@	@	@	@	@	@	@	@
		808017424794512875886459904961710757005754368000000000	8309562962452852382355161088000000	139511839126336328171520000	3765617127571985163878400	1429615077540249600	272237831663616000	3317504273309696000	26489012826931200	48704929136640	8244323942400	1365154560000000
		p power	A	A	A	A	A	B	A	B	B	A
		p' part	A	A	A	A	A	A	A	A	A	A
	Ind	1A	2A	2B	3A	3B	3C	4A	4B	4C	4D	5A
χ_1	+	1	1	1	1	1	1	1	1	1	1	1
χ_2	+	196883	4371	275	782	53	-1	275	51	19	-13	133
χ_3	+	21296876	91884	-2324	7889	-130	248	1772	-52	-20	12	626
χ_4	+	842609326	1139374	12974	55912	-221	-248	8878	782	-82	78	2451
χ_5	+	18538750076	8507516	123004	249458	1598	248	28796	2652	180	156	6326
χ_6	+	19360062527	9362495	-58305	297482	1508	-247	35903	-833	63	-65	8152
χ_7	+	293553734298	53981850	98970	1055310	-3927	3876	94874	1274	-102	-454	17423
χ_8	+	3879214937598	337044990	-690690	4751823	-4173	-3876	345598	-3874	-258	286	54473
χ_9	+	36173193327999	1354188159	2864511	12616074	18954	0	701823	20383	-897	351	91124
χ_{10}	+	125510727015275	3215883115	1219435	24688454	-25375	248	1223531	19499	-661	-1365	145275
χ_{11}	+	190292345709543	2814161895	10249191	17144568	-8073	27000	734183	22151	-281	-1209	78793
χ_{12}	+	222879856734249	3864186921	-7196631	26057022	11310	34503	1187881	-39831	1577	1001	132374
χ_{13}	+	1044868466775133	9223504989	-15756195	47292301	84448	31123	1762397	-46019	-2723	637	170258
χ_{14}	+	1109944460516150	9697078070	26155830	40851749	97733	61256	1379126	87126	4662	-1002	123025
χ_{15}	+	2374124840062976	22509162496	4100096	110509112	-1456	-61504	4100096	8192	4096	0	392976
χ_{16}	o	8980616927734375	-2720265625	39414375	1603525	200200	-116375	-9625	-20825	8295	1575	0
χ_{17}	o	8980616927734375	-2720265625	39414375	1603525	200200	-116375	-9625	-20825	8295	1575	0
χ_{18}	+	15178147608537368	72990279960	-29873896	255751145	33254	-30628	7620888	-44200	-2280	728	620368
χ_{19}	+	39660520552077425	128459630705	47061105	367316348	-227227	30380	9660529	82705	-3215	6097	712425
χ_{20}	+	60359800576579350	143552415510	71276310	371703759	-95718	120498	9004822	98294	-4074	1078	627475
χ_{21}	+	251098487132187500	336140827500	339995500	599239034	251810	-147250	11393900	512396	10860	4940	653125
χ_{22}	+	290568421805921077	444043629365	45093685	948362611	36400	-147497	20222773	-122059	4917	-7371	1269827
χ_{23}	+	336041615485626050	536115345090	-288233790	1087588073	-68263	61256	22648514	-153374	-2622	-4446	1397925
χ_{24}	+	2500435234254428856	1864421481144	319494840	2635262973	691236	116622	42900152	249016	-5448	-8008	2160231
χ_{25}	+	2986480825407204125	1612726090525	-385717475	1933299500	-57343	779495	28797725	-204867	7709	7293	1358500

For example take the 196883-dimensional irreducible. Its 2B-character is 275 and the 3B-character is 53. So we are looking for a dimension vector such that $a_1 + a_2 = 196883$, $a_1 - 275 = a_2$ and $b_1 + b_2 + b_3 = 196883$, $b_1 - 53 = b_2 = b_3$ giving us for that representation the dimension vector of the quiver above $(98579, 98304, 65663, 65610, 65610)$.

Okay, so for each of the 194 irreducibles S_i we have determined a dimension vector $(a_1(i), a_2(i); b_1(i), b_2(i), b_3(i))$, then standard quiver-representation theory asserts that the number of loops in the vertex corresponding to S_i is equal to

$$dim(S_i)^2 + 1 - a_1(i)^2 - a_2(i)^2 - b_1(i)^2 - b_2(i)^2 - b_3(i)^2$$

and that the number of arrows from vertex S_i to vertex S_j is equal to

$dim(S_i)dim(S_j) - a_1(i)a_1(j) - a_2(i)a_2(j) - b_1(i)b_1(j) - b_2(i)b_2(j) - b_3(i)b_3(j)$

This data then determines completely the $\mathbb{CM}$-bimodule $\mathfrak{m}/\mathfrak{m}^2$ and hence the structure of the completion $\widehat{\mathbb{C}PSL_{2\mathfrak{m}}}$ containing all information the Monster can gain from the modular group.

But then, one doesn't have to go for the full regular representation of the Monster. Any faithful permutation representation will do, so we might as well go for the one of minimal dimension.

That one is known to correspond to the largest maximal subgroup of the Monster which is known to be a two-fold extension $2.\mathbb{B}$ of the Baby-Monster. The corresponding permutation representation is of dimension 97239461142009186000 and decomposes into Monster-irreducibles

$S_1 \oplus S_2 \oplus S_4 \oplus S_5 \oplus S_9 \oplus S_{14} \oplus S_{21} \oplus S_{34} \oplus S_{35}$

(in standard Atlas-ordering) and hence repeating the arguments above we get a quiver on just 9 vertices! The actual numbers of loops and arrows (I forgot to mention this, but the quivers obtained are actually symmetric) obtained were found after laborious computations mentioned in the previous section and the details I'll make avalable here.

Anyone who can spot a relation between the numbers obtained and any other part of mathematics will obtain quantities of genuine (ie. non-Inbev) Belgian beer...

series 2

MOONSHINE

2.1 The secret of 163

On page 227 of Symmetry and the Monster, Mark Ronan tells the story of Conway and Norton computing the number of independent *mini j-functions* (McKay-Thompson series) arising from the Moonshine module. There are 194 distinct characters of the monster, but some of them give the same series reducing the number of series to 171. But, these are not all linearly independent. Mark Ronan writes :

"Conway recalls that, 'As we went down into the 160s, I said let's guess what number we will reach.' They guessed it would be 163 - which has a very special property in number theory - and it was! There is no explanation for this. We don't know whether it is merely a coincidence, or something more. The special property of 163 in number theory has intruiging consequences, among which is the fact that $e^{\pi\sqrt{163}} = 262537412640768743.99999999999925...$ is very close to being a whole number."

The corresponding footnote is a bit cryptic and doesn't explain this near miss integer.

Fig. 2.1: Leopold Kronecker

"This special feature also yields a fact, first noticed by Euler, that the formula $x^2 - x + 41$ gives prime numbers for all values of x between 1 and 40. The connection with 163 is that the solution to $x^2 - x + 41 = 0$ involves the square root of -163."

So, what is really going on?

The *modular j-function* has a power series expansion in $q = e^{2\pi i\tau}$ starting off as

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

and classifies complex elliptic curves up to isomorphism, or equivalently, two-dimensional integral lattices up to a complex scaling factor. A source of two-dimensional integral lattices is given by the *rings of integers* $\mathbb{Z}.1 + \mathbb{Z}.\tau$ in quadratic imaginary extensions of the rational numbers $\mathbb{Q}(\sqrt{-D})$. So, perhaps one might expect special properties of the j-value $j(\tau)$ whenever this ring of integers has special properties.

Leopold Kronecker discovered in 1857 the remarkable fact that the *modular j-function detects the class number of* $\mathbb{Q}(\sqrt{-D})$. Recall that the class-number is a finite number

measuring the amount by which the ring on integers $\mathbb{Z}.1 + \mathbb{Z}.\tau$ in $\mathbb{Q}(\sqrt{-D})$ fails to be a unique factorization domain. He proved :

The function-value $j(\tau)$ is an algebraic integer whose degree is the class number of the quadratic extension. In particular, if the ring of integers in $\mathbb{Q}(\sqrt{-D})$ satisfied unique factorization (or equivalently, is a principal ideal domain), then $j(\tau)$ is an integer!

Special instances of this theorem were already known. For example, the Gaussian integers $\mathbb{Z}.1+\mathbb{Z}.i$ satisfy unique factorization and Gauss knew already that $j(i) = 12^3 = 1728$. He even knew that

$$j(\tfrac{1}{2}(1+\sqrt{-163})) = (-640320)^3 = -262537412640768000$$

and because $\mathbb{Z}.1+\mathbb{Z}.\frac{1}{2}(1+\sqrt{-163})$ is the ring of integers in $\mathbb{Q}(\sqrt{-163})$ and as the absolute value of this j-value is near the value of $e^{\pi\sqrt{163}}$ we must be closing in on the solution of the riddle.

Charles Hermite noticed in 1859 this curious numerical consequence of Kronecker's theorem. For, if one takes $\tau = \frac{1}{2}(1+\sqrt{-163})$ and plugs this into the definition of $q = e^{2\pi i}$ one gets the tiny number $q = e^{\pi i - \pi\sqrt{163}} = -e^{-\pi\sqrt{163}}$ which is equal to -0.00000000000000000380898093700765233 82... So, all but the first two terms in the series expansion of $j(\tau)$ will be very small. For example $196884q = -0.0000000000074992740...$ and the next term $21493760q^2$ is already 0.00000000000000000000000031183868... and further terms will be even a lot smaller.

Combining this information with the Gauss-computed value of $j(\tau)$ we get that

$$(-640320)^3 = -e^{\pi\sqrt{163}} + 744 - \text{tiny number}$$

whence the observed curious approaximation of

$$e^{\pi\sqrt{163}} = 262537412640768000 + 744 - \text{tiny number} = 262537412640768743.99999999999925...$$

What about other near misses which follow from Kronecker's result? Unfortunately there are only nine imaginary quadratic extension $\mathbb{Q}(\sqrt{-D})$ for which the corresponding ring of integers satisfies unique factorization, namely

$$D = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

and of course the near misses will be worse for smaller values of D. For example for the next two largest values one calculates

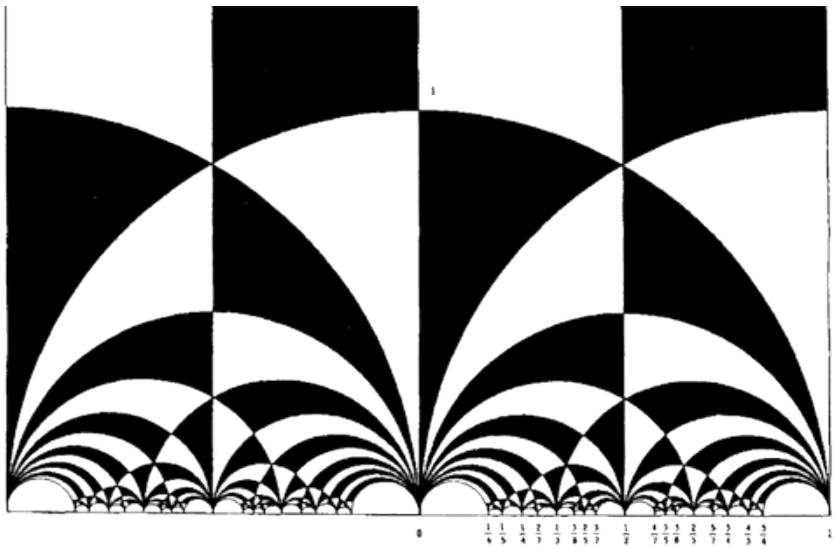
$$e^{\pi\sqrt{67}} = 147197952743.99999866245422...$$

$$e^{\pi\sqrt{43}} = 884736743.99977746603490661...$$

Fig. 2.2: Charles Hermite

Reference : John Stillwell, Modular Miracles, The American Mathematical Monthly, 108 (2001) 70-76

2.2 The Dedekind tessellation



In 1877, Richard Dedekind discovered one of the most famous pictures in mathematics : the black & white tessellation of the upper half-plane in hyperbolic triangles. Recall that the group $SL_2(\mathbb{Z})$ of all invertible 2x2 integer matrices with determinant 1 acts on the upper halfplane via

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}.z = \frac{az+b}{cz+d}$$

and as minus the identity matrix acts trivially, it is really an action of the *modular group* $\Gamma = PSL_2(\mathbb{Z})$. Any black or white triangle in the Dedekind-tessellation is a fundamental domain for the action of the *extended modular group* Γ^*, generated by Γ and the morphism $z \mapsto -\overline{z}$. . Dedekind showed that the union of any back and white region is a fundamental domain for the action of the modular group. For example, the 'usual' fundamental domain is the union of the top middle black and white regions in Dedekinds picture. Having this tessellation before you is essential if you have to wade through the heavy notation of the important paper by Ravi Kulkarni "An arithmetic-geometric method in the study of the subgroups of the modular group", which is what we aim to do now. Applications will be given in future posts in this series.

At some points (such as i) two black and two white regions are coming together, we call such points *even vertices* and they form the Γ^*-orbit of i. At other points (such as $\rho = e^{\frac{\pi i}{3}}$) three black and white regions are meeting and we call such points *odd vertices* (they form the Γ^*-orbit of ρ). The Γ^*-orbit of ∞ consists of the rational numbers and they are called the *cusps*.

Now, for the edges. There are three types of edges : *even edges* connecting a cusp and an even vertex (they form the Γ^*-orbit of the line (∞, i)), *odd edges* connecting a cusp to an odd vertex (the translates of (∞, ρ)) and finally *f-edges* (f for finite) connecting an odd and even vertex (the Γ^*-orbit of the arc (ρ, i)).

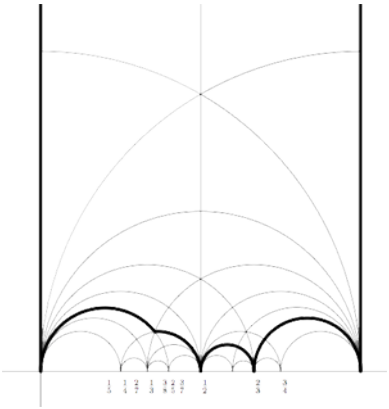
The geodesics (the semi-circles and the vertical lines) are made of edges and they come in two types : *even lines* are complete geodesics which are unions of two even edges (such as the semi-circle $(0, 1)$) and *odd lines* (such as the semi-circle $(-1, 1)$) are complete geodesics which are unions of two f-edges and two odd edges. Remark that the vertical lines are even if they pass through an integer and odd when they go through a half-integer. The modular group Γ acts transitively on the even (resp. odd) lines.

If we write rational numbers in reduced form $\frac{a}{b}$ (and if we agree to write integers as $\frac{n}{1}$ and $\infty = \frac{1}{0}$) then, if a geodesic has endpoints $\frac{a}{b}$ and $\frac{c}{d}$ it is an even line iff $|ad - bc| = 1$ and an odd line iff $|ad - bc| = 2$.

This notation was set up to define the notion of a *special polygon* which is a connected polygonal region P in the upper-halfplane such that its boundary ∂P consists entirely of even and odd edges (so *no f-edges*) together with a side-pairing satisfying the following requirements

1. Even edges in ∂P come in pairs and each such pair forms an even line.
2. Odd edges in ∂P come in pairs and each pair meets at an odd vertex where they make an internal angle of $\frac{2\pi}{3}$.
3. Any odd edge e is side-paired to a different odd edge f which makes on internal angle $\frac{2\pi}{3}$ with e.
4. If e and f are even edges in ∂P forming an even line, then either e is side-paired to f or else e,f form a **free side** and is side-paired to a different such free side.
5. $0, \infty$ are among the vertices of P.

The *sides* of P are : the odd edges on the boundary, the free sides and the even edges on non-free sides. The *vertices* of P are the intersections of adjacent sides.



For example, the region inside the thick edges is a special polygon. Its boundary consists of 8 even edges (two on the 4 complete geodesics : the vertical lines at 0 and 1 and the semi-circles $(\frac{1}{2}, \frac{2}{3})$ and $(\frac{2}{3}, 1)$) and 2 odd edges the arc-fragments in the lower left corner, the leftmost being part of the semi-circle $(0, \frac{1}{3})$, the other part of the semi-circle $(\frac{1}{4}, \frac{1}{2})$.

We have several option for the side-pairing, the only forded pairing being the two odd edges which have to be paired. For the even edges we can either consider 0,2 or 4 of the geodesics as free sides and pair these, or we can have 0,2 or 4 non-free sides and then we have to pair up the two even edges making such a non-free side.

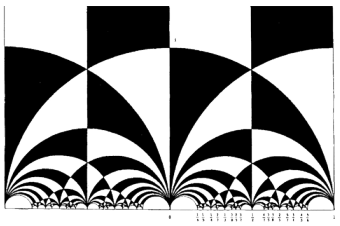
The number of sides of the special polygon depends on the number of free sides chosen. For 0 free sides, there are 10 sides and vertices. For 2 free sides, there are 8 sides and vertices and for 4 free sides we have 6 sides and vertices.

Special polygons are a combinatorial gadget to describe the subgroups of finite index in the modular group $PSL_2(\mathbb{Z})$. Later, we will connect this notion to *quilts* which are special 'dessins d'enfants' and to generalized *Farey sequences*. This will then allow us to find explicit generators of the subgroups.

Some technical issues : if some of the latex-pictures don't show up nicely it often helps to resize the browser-window and resize it back. The drawing of the special polygon was made using the LaTeX-package MFPIC which is an easy to use interface to MetaPost.

Reference : Ravi S. Kulkarni "An arithmetic-geometric method in the study of the subgroups of the modular group" Amer. J. Math. 113 (1991) 1053-1133

2.3 Dedekind or Klein?



The black and white psychedelic picture on the left of a tessellation of the hyperbolic upper-halfplane, we called the *Dedekind tessellation*, following the reference given by John Stillwell in his excellent paper Modular Miracles, The American Mathematical Monthly, 108 (2001) 70-76.

But is this correct terminology? Nobody else uses it according to Google. So, let's try to track down the earliest depiction of this tessellation in the literature...

Stillwell refers to Richard Dedekind's 1877 paper "Schreiben an Herrn Borchard uber die Theorie der elliptische Modulfunktionen", which appeared beginning of september 1877 in Crelle's journal (Journal fur die reine und angewandte Mathematik, Bd. 83, 265-292).

Fig. 2.3: Richard Dedekind

There are a few odd things about this paper. To start, it really is the transcript of a (lengthy) letter to Herrn Borchardt (at first, I misread the recipient as Herrn Borcherds which would be really weird...), written on June 12th 1877, just 2 and a half months before it appeared... Even today in the age of camera-ready-copy it would probably take longer.

There isn't a single figure in the paper, but, it is almost impossible to follow Dedekind's arguments without having a mental image of the tessellation. He gives a fundamental domain for the action of the modular group $\Gamma = PSL_2(\mathbb{Z})$ on the hyperbolic upper-half plane (a fact already known to Gauss) and goes on in section 3 to give a one-to-one mapping between this domain and the complex plane using what he calls the 'valenz' function v (which is our modular function j, making an appearance in moonshine, and responsible for the black and white tessellation, the two colours corresponding to pre-images of the upper or lower half-planes).

Then there is this remarkable opening sentence.

"Sie haben mich aufgefordert, eine etwas ausfuhrlichere Darstellung der Untersuchungen auszuarbeiten, von welchen ich, durch das Erscheinen der Abhandlung von Fuchs veranlasst, mir neulich erlaubt habe Ihnen eine kurze Ubersicht mitzuteilen; indem ich Ihrer Einladung hiermit Folge leiste, beschranke ich mich im wesentlichen auf den Teil dieser Untersuchungen, welcher mit der eben genannten Abhandlung zusammenhangt, und ich bitte Sie auch, die Ubergehung einiger Nebenpunkte entschuldigen zu wollen, da es mir im Augenblick an Zeit fehlt, alle Einzelheiten auszufuhren."

Well, just try to get a paper (let alone a letter) accepted by Crelle's Journal with an opening line like : "I'll restrict to just a few of the things I know, and even then, I cannot be bothered to fill in details as I don't have the time to do so right now!" But somehow, Dedekind got away with it.

So, who was this guy Borchardt? How could this paper be published so swiftly? And, what might explain this extreme 'je m'en fous'-opening ?

Carl Borchardt was a Berlin mathematician whose main claim to fame seems to be that he succeeded Crelle in 1856 as main editor of the 'Journal fur reine und...' until 1880 (so in 1877 he was still in charge, explaining the swift publication). It seems that during this time the 'Journal' was often referred to as "Borchardt's Journal" or in France as "Journal de M Borchardt". After Borchardt's death, the Journal für die Reine und Angewandte Mathematik again became known as Crelle's Journal.

As to the opening sentence, I have a toy-theory of what was going on. In 1877 a bitter dispute was raging between Kronecker (an editor for the Journal and an important one as he was the one succeeding Borchardt when he died in 1880) and Cantor. Cantor had published most of his papers at Crelle and submitted his latest find : there is a one-to-one correspondence between points in the unit interval [0,1] and points of d-dimensional space! Kronecker did everything in his power to stop that paper to the extend that Cantor wanted to retract it and submit it elsewhere. Dedekind supported Cantor and convinced him not to retract the paper and used his influence to have the paper published in Crelle in 1878. Cantor greatly resented Kronecker's opposition to his work and never submitted any further papers to Crelle's Journal.

Fig. 2.4: Carl Borchardt

Clearly, Borchardt was involved in the dispute and it is plausible that he 'invited' Dedekind to submit a paper on his old results in the process. As a further peace offering, Dedekind included a few 'nice' words for Kronecker

"Bei meiner Versuchen, tiefer in diese mir unentbehrliche Theorie einzudringen und mir einen einfachen Weg zu den ausgezeichnet schonen Resultaten von Kronecker zu bahnen, die leider noch immer so schwer zuganglich sind, enkannte ich sogleich..."

Probably, Dedekind was referring to Kronecker's relation between class groups of quadratic imaginary fields and the j-function, see *the miracle of 163*. As an added bonus, Dedekind was elected to the Berlin academy in 1880...

Anyhow, no visible sign of 'Dedekind's' tessellation in the 1877 Dedekind paper, so, we have to look further. I'm fairly certain to have found the earliest depiction of the black and white tessellation (if you have better info, please drop a line). Here it is

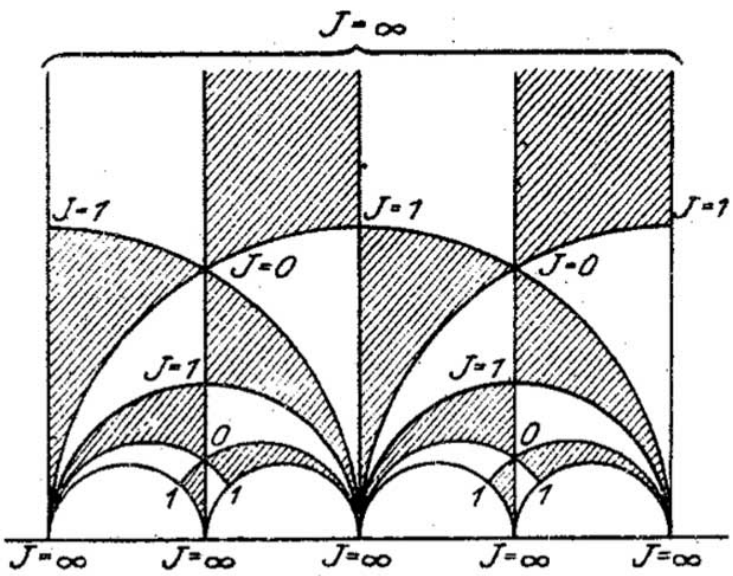


Fig. 7.

It is figure 7 in Felix Klein's paper "Uber die Transformation der elliptischen Funktionen und die Auflosung der Gleichungen funften Grades" which appeared in may 1878 in the Mathematische Annalen (Bd. 14 1878/79). He even adds the j-values which make it clear why black triangles should be oriented counter-clockwise and white triangles clockwise. If Klein would still be around today, I'm certain he'd be a metapost-guru.

So, perhaps the tessellation should be called Klein's tessellation?? Well, not quite. Here's what Klein writes wrt. figure 7

" Diese Figur nun - welche die eigentliche Grundlage fur das Nachfolgende abgibt - ist eben diejenige, von der Dedekind bei seiner Darstellung ausgeht. Er kommt zu ihr durch rein arithmetische Betrachtung."

Case closed : Klein clearly acknowledges that Dedekind did have this picture in mind when writing his 1877 paper!

But then, there are a few odd things about Klein's paper too, and, I do have a toy-theory about this as well... (tbc)

2.4 Monsieur Mathieu

Take your favourite $SL_2(\mathbb{Z})$-representation. Here is mine : the permutation presentation of the Mathieu group(s). Emile Leonard Mathieu is remembered especially for his discovery (in 1861 and 1873) of five sporadic simple groups named after him, the Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}$ and M_{24}. These were studied in his thesis on transitive functions.

He had a refreshingly direct style of writing. I'm not sure what Cauchy would have thought (Cauchy died in 1857) about this 'acknowledgement' in his 1861-paper in which Mathieu describes M_{12} and claims the construction of M_{24}.

tions. Je rappellerai encore que, malgré le petit nombre de résultats acquis à cette doctrine, Cauchy avait publié pendant le cours de l'année 1845, dans les *Comptes rendus des séances de l'Académie*, une longue série de Mémoires entièrement relatifs à cette théorie, mais il ne fit la découverte d'aucune fonction.

A ces Mémoires de Cauchy j'ai toutefois emprunté une idée, et une seule : c'est celle de distinguer les fonctions en fonctions transitives et en fonctions intransitives. En effet, dans cette théorie, ce sont les fonctions transitives, et surtout celles qui le sont plusieurs fois, qui sont seules vraiment remarquables.

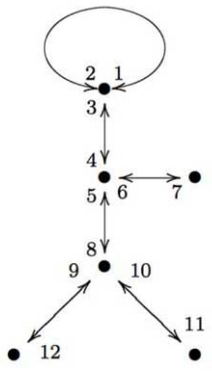
Also the opening sentenses of his 1873 paper are nice, something along the lines of "if no expert was able to fill in the details of my claims made twelve years ago, I'd better do it myself".

Dans mon Mémoire *sur les fonctions de plusieurs quantités* publié dans le tome VI de ce Journal, en 1861, j'ai déclaré (p. 274) que je possédais une fonction cinq fois transitive de 24 quantités, dont j'ai donné en même temps le nombre des valeurs distinctes.

Si j'avais indiqué deux substitutions qui la laissent invariable et qui la caractérisent complétement, il eût été facile de vérifier son existence; mais, au contraire, la seule indication du nombre de ses valeurs distinctes ne jette aucune lumière sur la formation de cette fonction. Aussi aucun géomètre n'a-t-il essayé, depuis cette époque, de la déterminer, et je me propose maintenant de prouver qu'elle existe effectivement et de montrer, de plus, comment je suis parvenu à la découvrir.

However, even after this paper opinions remained divided on the issue whether or not he did really achieve his goal, and the matter was settled decisively by Ernst Witt connecting the Mathieu groups to Steiner systems (if I recall well from Mark Ronan's book Symmetry and the monster)

As Mathieu observed, the quickest way to describe these groups would be to give generators, but as these groups are generated by two permutations on 12 respectively 24 elements, we need to have a mnemotechnic approach to be able to reconstruct them whenever needed.



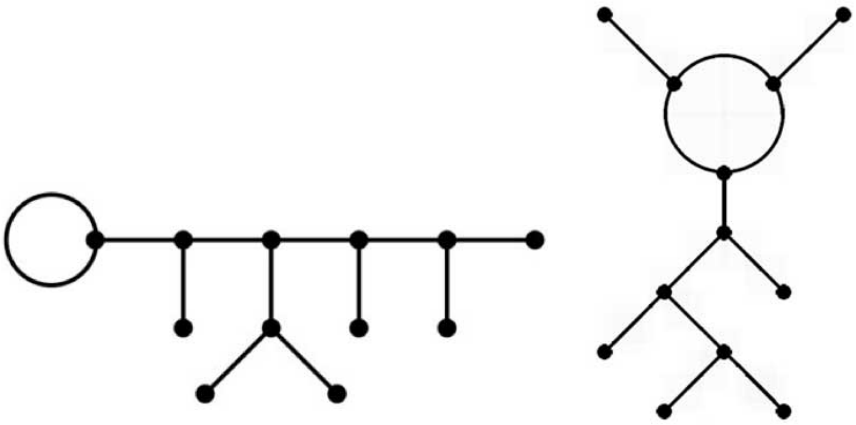
Here is a nice approach, due to Gunther Malle in a Luminy talk in 1993 on "Dessins d'enfants" (more about them later). Consider the drawing of "Monsieur Mathieu" on the left. That is, draw the left-handed bandit picture on 6 edges and vertices, divide each edge into two and give numbers to both parts (the actual numbering is up to you, but for definiteness let us choose the one on the left). Then, M_{12} is generated by the order two permutation describing the labeling of both parts of the edges

$$s = (1,2)(3,4)(5,8)(7,6)(9,12)(11,10)$$

together with the order three permutation obtained from cycling counterclockwise around a trivalent vertex and calling out the labels one encounters. For example, the three cycle corresponding to the 'neck vertex' is $(1,2,3)$ and the total permutation is

$$t = (1,2,3)(4,5,6)(8,9,10)$$

A quick verification using GAP tells that these elements do indeed generate a simple group of order 95040.



Similarly, if you have to reconstruct the largest Mathieu group from scratch, apply the same method to the the pictures above, copied from Alexander Zvonkin's paper How to draw a group as well as the computational details below.

This is all very nice and well but what do these drawings have to do with Grothendieck's "dessins d'enfants"? Consider the map from the projective line onto itself

$\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$

defined by the rational map

$f(z) = \frac{(z^3-z^2+az+b)^3(z^3+cz^2+dz+e)}{Kz}$

where N. Magot calculated that

$a = \frac{107+7\sqrt{-11}}{486}, b = -\frac{13}{567}a + \frac{5}{1701}, c = -\frac{17}{9}, d = \frac{23}{7}a + \frac{256}{567}, e = -\frac{1573}{567}a + \frac{605}{1701}$

and finally

$K = -\frac{16192}{301327047}a + \frac{10880}{903981141}$

One verifies that this map is 12 to 1 everywhere except over the points $0, 1, \infty$ (that is, there are precisely 12 points mapping under f to a given point of $\mathbb{P}^1_{\mathbb{C}} - 0, 1, \infty$. From the expression of f(z) it is clear that over 0 there lie 6 points (3 of which with multiplicity three, the others of multiplicity one). Over ∞ there are two points, one with multiplicity 11 and one with multiplicity one. The difficult part is to compute the points lying over 1. The miraculous fact of the given values is that

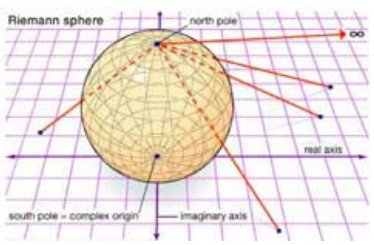
$f(z) - 1 = \frac{-B(z)^2}{Kz}$

with

$B(z) = z^6 + \frac{1}{11}(10c - 8)z^5 + (5a + 9d - 7c)z^4$

$+(2b + 4ac + 8e - 6d)z^3 + (3ad + bc - 5e)z^2 + 2aez - be)$

and hence there are 6 points lying over 1 each with mutiplicity two.



Right, now consider the complex projective line $\mathbb{P}^1_{\mathbb{C}}$ as the Riemann sphere S^2 and mark the six points lying over 1 by a white vertex and the six points lying over 0 with a black vertex (in the source sphere).

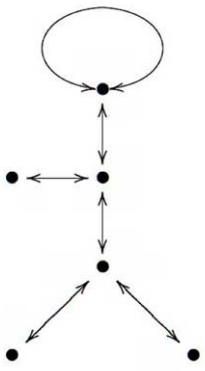
Now, lift the real interval $[0, 1]$ in the target sphere $\mathbb{P}^1_{\mathbb{C}} = S^2$ to its inverse image on the source sphere.

As there are exactly 12 points lying over each real number $0 \lneq r \lneq 1$, this inverse image will consist of 12 edges which are noncrossing and each end in one black and one white vertex.

The obtained graph will look like the "Monsieur Mathieu" drawing above with the vertices corresponding to the black vertices and the three points over 1 of multiplicity three corresponding to the trivalent vertices, those of multiplicity one to the three end-vertices. The white vertices correspond to mid-points of the six edges, so that we do get a drawing with twelve edges, one corresponding to each number.

From the explicit description of f(z) it is clear that this map is defined over $\mathbb{Q}\sqrt{-11}$ which is also the smallest field containing all character-values of the Mathieu group M_{12}. Further, the Galois group of the extension $Gal(\mathbb{Q}\sqrt{-11}/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ and is generated by complex conjugation. So, one might wonder what would happen if we replaced in the definition of the rational map f(z) the value of a by $a = \frac{107-\sqrt{-11}}{486}$.

It turns out that this modified map has the same properties as $f(z)$ so again one can draw on the source sphere a picture consisting of twelve edges each ending in a white and black vertex.



If we consider the white vertices (which incidentally each lie on two edges as all points lying over 0 are of multiplicity two) as mid-points of longer edges connecting the black vertices we obtain a drawing on the sphere which looks like "Monsieur Mathieu" but this time as a right handed bandit, and applying our mnemotechnic rule we obtain *another* (non conjugated) embedding of M_{12} in the full symmetric group on 12 vertices.

What is the connection with $SL_2(\mathbb{Z})$-representations? Well, the permutation generators s and t of M_{12} (or M_{24} for that matter) have orders two and three, whence there is a projection from the free group product $C_2 \star C_3$ (here C_n is just the cyclic group of order n) onto M_{12} (respectively M_{24}).

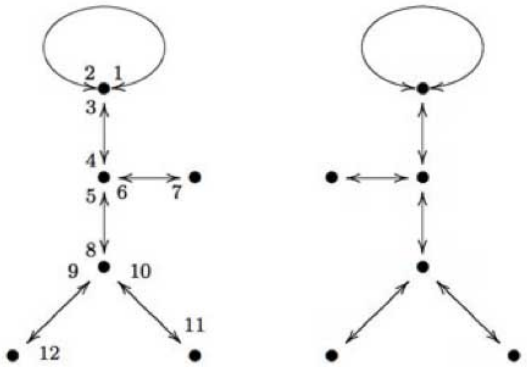
We will say more about such free group products and show (among other things) that $PSL_2(\mathbb{Z}) \simeq C_2 \star C_3$ whence the connection with $SL_2(\mathbb{Z})$. Further on, we will extend the Monsieur Mathieu example to arbitrary dessins dénfants which will allow us to assign to curves defined over $\overline{\mathbb{Q}}$ permutation representations of $SL_2(\mathbb{Z})$ and other *cartographic groups* such as the congruence subgroups $\Gamma_0(2)$ and $\Gamma(2)$.

2.5 The best rejected research proposal, ever

The Oscar in the category *The Best Rejected Research Proposal in Mathematics (ever)* goes to ... Alexander Grothendieck for his proposal Esquisse d'un Programme, Grothendieckś research program from 1983, written as part of his application for a position at the CNRS, the French equivalent of the NSF. An English translation is available.

Here is one of the problems discussed : *Give TWO non-trivial elements of* $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ the *absolute* Galois group of the algebraic closure of the rational numbers $\overline{\mathbb{Q}}$, that is the group of all $\mathbb{Q}$-automorphisms of $\overline{\mathbb{Q}}$. One element most of us can give (complex-conjugation) but to find any other element turns out to be an extremely difficult task.

To get a handle on this problem, Grothendieck introduced his *'Dessins d'enfants'* (Children's drawings). Recall from the last section the pictures of the left and right handed Monsieur Mathieu



The left hand side drawing was associated to a map $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ which was defined over the field $\mathbb{Q}\sqrt{-11}$ whereas the right side drawing was associated to the map given when one applies to all coefficients the unique non-trivial automorphism in the Galois group $Gal(\mathbb{Q}\sqrt{-11}/\mathbb{Q})$ (which is complex-conjugation).

Hence, the Galois group $Gal(\mathbb{Q}\sqrt{-11}/\mathbb{Q})$ acts *faithfully* on the drawings associated to maps $\mathbb{P}^1_{\mathbb{Q}\sqrt{-11}} \to \mathbb{P}^1_{\mathbb{Q}\sqrt{-11}}$ which are ramified only over the points $0, 1, \infty$.

Grothendieck's idea was to extend this to more general maps. Assume that a projective smooth curve (a Riemann surface) X is defined over the algebraic numbers $\overline{\mathbb{Q}}$ and *assume* that there is a map $X \to \mathbb{P}^1_{\mathbb{C}}$ ramified only over the points $0, 1, \infty$, then we can repeat the procedure of last time and draw a picture on X consisting of d edges (where d is the degree of the map, that is the number of points lying over another point of $\mathbb{P}^1_{\mathbb{C}}$) between white resp. black points (the points of X lying over 1 (resp. over 0)).

Call such a drawing a *'dessin dénfant'* and look at the collection of ALL dessins d'enfants associated to ALL such maps where X runs over ALL curves defined over $\overline{\mathbb{Q}}$. On this set, there is an action of the *absolute Galois group* $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ and if this action would be faithful, then this would give us insight into this group. However, at that time even the existence of a map $X \to \mathbb{P}^1$ ramified in the three points $0, 1, \infty$ seemed troublesome to prove, as Grothendieck recalls in his proposal

"In more erudite terms, could it be true that every projective non-singular algebraic curve defined over a number field occurs as a possible modular curve parametrising elliptic curves equipped with a suitable rigidification? Such a supposition seemed so crazy that I was almost embarrassed to submit it to the competent people in the domain. Deligne when I consulted him found it crazy indeed, but didn't have any counterexample up his sleeve. Less than a year later, at the International Congress in Helsinki, the Soviet mathematician Bielyi announced exactly that result, with a proof of disconcerting simplicity which fit into two little pages of a letter of Deligne never, without a doubt, was such a deep and disconcerting result proved in so few lines!

" In the form in which Bielyi states it, his result essentially says that every algebraic curve defined over a number field can be obtained as a covering of the projective line ramified only over the points 0, 1 and infinity. This result seems to have remained more or less unobserved. Yet, it appears to me to have considerable importance. To me, its essential message is that there is a profound identity between the combinatorics of finite maps on the one hand, and the geometry of algebraic curves defined over number fields on the other.

This deep result, together with the algebraic- geometric interpretation of maps, opens the door onto a new, unexplored world within reach of all, who pass by without seeing it. ”

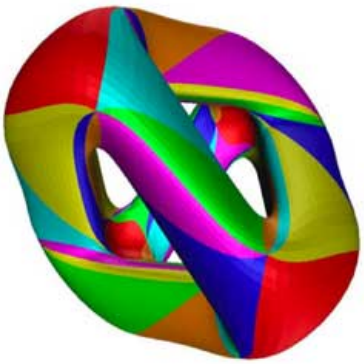
Belyi's proof is indeed relatively easy (full details can be found in the paper Dessins d'enfants on the Riemann sphere by Leila Schneps). Roughly it goes as follows : as both X and the map are defined over $\overline{\mathbb{Q}}$ the map is only ramified over (finitely many) $\overline{\mathbb{Q}}$-points. Let S be the finite set of all Galois-conjugates of these points and consider the polynomial

$f_0(z_0) = \prod_{s \in S}(z_0 - s) \in \mathbb{Q}[z_0]$

Now, do a resultant trick. Consider the polynomial $f_1(z_1) = Res_{z_0}(\frac{df_0}{dz_0}, f_0(z_0) - z_1)$ then the roots of $f_1(z_1)$ are exactly the finite critical values of f_0, f_1 is again defined over $\mathbb{Q}$ and has lower degree (in z_1) than f_0 in z_1. Continue this trick a finite number of times untill you have constructed a polynomial $f_n(z_n) \in \mathbb{Q}[z_n]$ of degree zero.

Composing the original map with the maps f_j in succession yields that all ramified points of this composition are $\mathbb{Q}$-points! Now, we only have to limit the number of these ramified $\mathbb{Q}$-points (let us call this set T) to three.

Take any three elements of T, then there always exist integers $m, n \in \mathbb{Z}$ such that the three points go under a linear fractional transformation (a Moebius-function associated to a matrix in $PGL_2(\mathbb{Q})$) to $0, \frac{m}{m+n}, 1$. Under the transformation $z \to \frac{(m+n)^{m+n}}{m^m n^n} z^m (1 - z)^n$ the points 0 and 1 go to 0 and $\frac{m}{m+n}$ goes to 1 whence the ramified points of the composition are one less in number than T. Continuing in this way we can get the set of ramified $\mathbb{Q}$-points of a composition at most having three elements and then a final Moebius transformation gets them to $0, 1, \infty$, done!

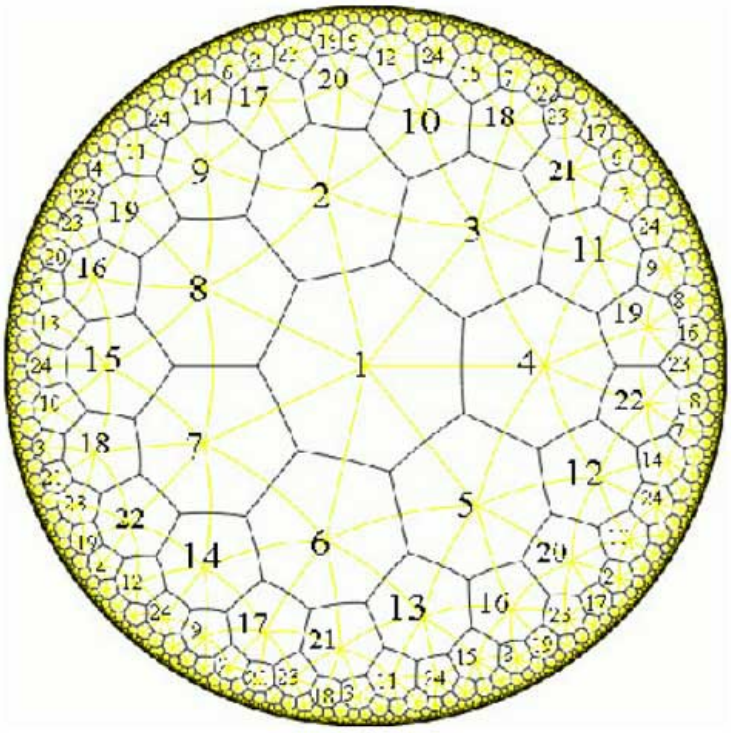


As a tribute for this clever argument, maps $X \to \mathbb{P}^1$ ramified only in 0,1 and ∞ are now called *Belyi morphisms*. Here is an example of a Belyi-morphism (and the corresponding dessin d'enfants) associated to one of the most famous higher genus curves around : the Klein quartic (if you haven't done so yet, take your time to go through this marvelous pre-blog post by John Baez).

One can define the Klein quartic as the plane projective curve K with defining equation in $\mathbb{P}^2_{mathbbC}$ given by $X^3Y + Y^3Z + Z^3X = 0$ K has a large group of automorphism, namely the simple group of order 168 $G = PSL_2(\mathbb{F}_7) = SL_3(\mathbb{F}_2)$.

It is a classical fact (see for example the excellent paper by Noam Elkies The Klein quartic in number theory) that the quotient map $K \to K/G = \mathbb{P}^1_{\mathbb{C}}$ is ramified only in the points 0,1728 and ∞ and the number of points of K lying over them are resp. 56, 84 and 24.

Now, compose this map with the Moebius transformation taking $0, 1728, \infty \to 0, 1, \infty$ then the resulting map is a Belyi-map for the Klein quartic. A topological construction of the Klein quartic is fitting 24 heptagons together so that three meet in each vertex, see below for the gluing data-picture in the hyperbolic plane : the different heptagons are given a number but they appear several times telling how they must fit together)



The resulting figure has exactly $\frac{7\times 24}{2} = 84$ edges and the 84 points of K lying over 1 (the white points in the dessin) correspond to the midpoints of the edges. There are exactly $\frac{7\times 24}{3} = 56$ vertices corresponding to the 56 points lying over 0 (the black points in the dessin).

Hence, the dessin dénfant associated to the Klein quartic is the figure traced out by the edges on K. Giving each of the 168 half-edges a different number one assigns to the white points a permutation of order two and to the three-valent black-points a permutation of order three, whence to the Belyi map of the Klein quartic corresponds a 168-dimensional permutation representation of $SL_2(\mathbb{Z})$, which is not so surprising as the group of automorphisms is $PSL_2(\mathbb{F}_7)$ and the permutation representation is just the regular representation of this group.

Further on, we will see how one can always associate to a curve defined over $\overline{\mathbb{Q}}$ a permutation representation (via the Belyi map and its dessin) of one of the congruence subgroups $\Gamma(2)$ or $\Gamma_0(2)$ or of $SL_2(\mathbb{Z})$ itself.

2.6 The cartographer's groups (1/2)

Just as cartographers like Mercator drew maps of the then known world, we draw *dessins d 'enfants* to depict the associated algebraic curve defined over $\overline{\mathbb{Q}}$.

In order to see that such a dessin d'enfant determines a permutation representation of one of Grothendieck's *cartographic groups*, $SL_2(\mathbb{Z}), \Gamma_0(2)$ or $\Gamma(2)$ we need to have realizations of these groups (as well as their close relatives $PSL_2(\mathbb{Z}), GL_2(\mathbb{Z})$ and $PGL_2(\mathbb{Z})$) in terms of generators and relations.

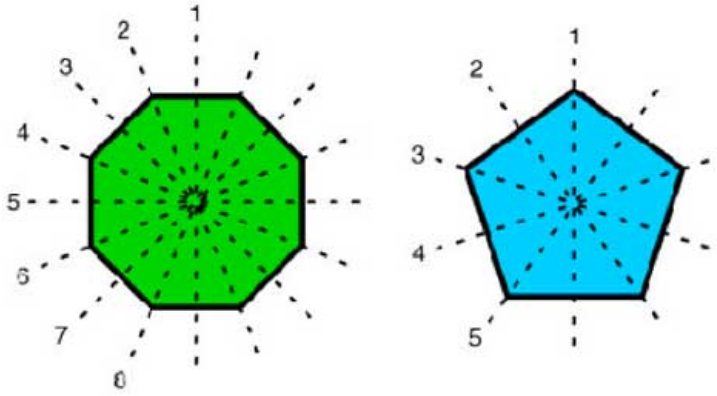
As this will be rather technical I'd better first explain what we will prove (so that you can skip it if you feel comfortable with the statements) and why we want to prove it. What we will prove in detail below is that these groups can be written as *free (or amalgamated) group products*. We will explain what this means and will establish that

$PSL_2(\mathbb{Z}) = C_2 * C_3, \Gamma_0(2) = C_2 * C_\infty, \Gamma(2) = C_\infty * C_\infty$

$SL_2(\mathbb{Z}) = C_4 *_{C_2} C_6, GL_2(\mathbb{Z}) = D_4 *_{D_2} D_6, PGL_2(\mathbb{Z}) = D_2 *_{C_2} D_3$

where C_n resp. D_n are the *cyclic* (resp. *dihedral*) groups. The importance of these facts it that they will allow us to view the set of (isomorphism classes of) finite dimensional representations of these groups as *noncommutative manifolds* . Looking at the statements above we see that these arithmetical groups can be build up from the first examples in any course on finite groups : cyclic and dihedral groups.

Recall that the cyclic group of order n, C_n is the group of rotations of a regular n-gon (so is generated by a rotation r with angle $\frac{2\pi}{n}$ and has defining relation $r^n = 1$, where 1 is the identity). However, regular n-gons have more symmetries : flipping over one of its n lines of symmetry



The dihedral group D_n is the group generated by the n rotations and by these n flips. If, as before r is a generating rotation and d is one of the flips, then it is easy to see that the dihedral group is generated by r and d and satisfied the defining relations

$r^n = 1$ and $d^2 = 1 = (rd)^2$

Flipping twice does nothing and to see the relation $(rd)^2 = 1$ check that doing twice a rotation followed by a flip brings all vertices back to their original location. The dihedral group D_n has 2n elements, the n-rotations r^i and the n flips dr^i.

In fact, to get at the cartographic groups we will only need the groups D_4, D_6 and their subgroups. Let us start by finding generators of the largest group $GL_2(\mathbb{Z})$ which is the group of all invertible 2×2 matrices with integer coefficients.

Consider the elements

$$U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, V = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \text{ and } R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and form the matrices

$$X = UV = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, Y = VU = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

By induction we prove the following relations in $GL_2(\mathbb{Z})$

$$X^n \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a-nc & b-nd \\ c & d \end{bmatrix} \text{ and } \begin{bmatrix} a & b \\ c & d \end{bmatrix} X^n = \begin{bmatrix} a & b-na \\ c & d-nc \end{bmatrix}$$

$$Y^n \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c+na & d+nb \end{bmatrix} \text{ and } \begin{bmatrix} a & b \\ c & d \end{bmatrix} Y^n = \begin{bmatrix} a+nb & b \\ c+nd & d \end{bmatrix}$$

The determinant ad-bc of a matrix in $GL_2(\mathbb{Z})$ must be ± 1 whence all rows and columns of

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z})$$

consist of coprime numbers and hence a and c can be reduced modulo each other by left multiplication by a power of X or Y until one of them is zero and the other is ± 1. We may even assume that $a = \pm 1$ (if not, left multiply with U).

So, by left multiplication by powers of X and Y and U we can bring any element of $GL_2(\mathbb{Z})$ into the form

$$\begin{bmatrix} \pm 1 & \beta \\ 0 & \pm 1 \end{bmatrix}$$

and again by left multiplication by a power of X we can bring it in one of the four forms

$$\begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix} = 1, UR, RU, U^2$$

This proves that $GL_2(\mathbb{Z})$ is generated by the elements U,V and R.

Similarly, the group $SL_2(\mathbb{Z})$ of all 2×2 integer matrices with determinant 1 is generated by the elements U and V as using the above method and the restriction on the determinant we will end up with one of the two matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = 1, U^2$$

so we never need the matrix R. As for relations, there are some obvious relations among the matrices U,V and R, namely

$U^2 = V^3$ and $1 = U^4 = R^2 = (RU)^2 = (RV)^2$

The real problem is to prove that all remaining relations are consequences of these basic ones. As R clearly has order two and its commutation relations with U and V are just $RU = U^{-1}R$ and $RV = V^{-1}R$ we can pull R in any relation to the far right and (possibly after multiplying on the right with R) are left to prove that the only relations among U and V are consequences of $U^2 = V^3$ and $U^4 = 1 = V^6$.

Because $U^2 = V^3$ this element is central in the group generated by U and V (which we have seen to be $SL_2(\mathbb{Z})$) and if we quotient it out we get the **modular group**

$\Gamma = PSL_2(\mathbb{Z})$

Hence in order to prove our claim it suffices that

$PSL_2(\mathbb{Z}) = \langle \overline{U}, \overline{V} : \overline{U}^2 = \overline{V}^3 = 1 \rangle$

Phrased differently, we have to show that $PSL_2(\mathbb{Z})$ is the **free group product** of the cyclic groups of order two and three (those generated by $u = \overline{U}$ and $v = \overline{V}$) $C_2 * C_3$

Any element of this free group product is of the form $(u)v^{a_1}uv^{a_2}u \dots uv^{a_k}(u)$ where beginning and trailing u are optional and all a_i are either 1 or 2.

So we have to show that in $PSL_2(\mathbb{Z})$ no such word can give the identity element. We will first sketch the classical argument based on the theory of groups acting on trees due to Jean-Pierre Serre and Hyman Bass.

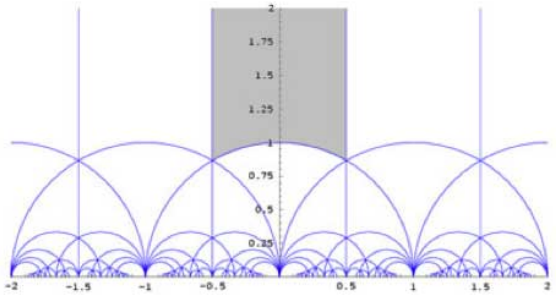
In the next section, we will give a short elegant proof due to Roger Alperin and draw consequences to the description of the carthographic groups as *amalgamated free products* of cyclic and dihedral groups.

Recall that $GL_2(\mathbb{Z})$ acts via Moebius transformations on the complex plane $\mathbb{C} = \mathbb{R}^2$ (actually it is an action on the Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$) given by the maps

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}.z = \frac{az+b}{cz+d}$$

Note that the action of the center of $GL_2(\mathbb{Z})$ (that is of $\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$) acts trivially, so it is really an action of $PGL_2(\mathbb{Z})$.

As R interchanges the upper and lower half-plane we might as well restrict to the action of $SL_2(\mathbb{Z})$ on the upper-halfplane $\mathcal{H}$. It is quite easy to see that a fundamental domain for this action is given by the greyed-out area

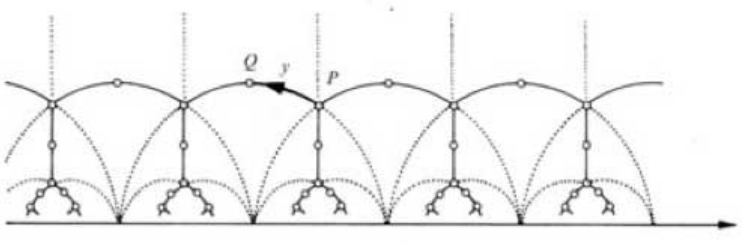


To see that any $z \in \mathcal{H}$ can be taken into this region by an element of $PSL_2(\mathbb{Z})$ note the following two Moebius transformations

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.z = z+1 \text{ and } \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.z = -\frac{1}{z}$$

The first operation takes any z into a strip of length one, for example that with Re(z) between $-\frac{1}{2}$ and $\frac{1}{2}$ and the second interchanges points within and outside the unit-circle, so combining the two we get any z into the greyed-out region. Actually, we could have taken any of the regions in the above tiling as our fundamental domain as they are all translates of the greyed-out region by an element of $PSL_2(\mathbb{Z})$.

Of course, points on the boundary of the greyed-out fundamental region need to be identified (in order to get the identification of $\overline{\mathcal{H}/PSL_2(\mathbb{Z})}$ with the Riemann sphere $S^2 = \mathbb{P}^1_{\mathbb{C}}$). For example, the two halves of the boundary by the unit circle are interchanged by the action of the map $z \to -\frac{1}{z}$ and if we take the translates under $PSL_2(\mathbb{Z})$ of the indicated circle-part



we get a connected tree with fundamental domain the circle part bounded by i and $\rho = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. Calculating the *stabilizer subgroup* of i (that is, the subgroup of elements fixing i) we get that this subgroup is $\langle u \rangle = C_2$ whereas the stabilizer subgroup of ρ is $\langle v \rangle = C_3$.

Using this facts and the general results of Jean-Pierre Serres book Trees one deduces that $PSL_2(\mathbb{Z}) = C_2 * C_3$ and hence that the obvious relations among U,V and R given above do indeed generate all relations.

2.7 The cartographer's groups (2/2)

Fortunately, there is a drastic shortcut to the general tree-argument of the previous section, due to Roger Alperin. Recall that the Moebius transformations corresponding to u resp. v send z resp. to

$-\frac{1}{z}$ and $\frac{1}{1-z}$

whence the Moebius transformation corresponding to v^{-1} send z to $1 - \frac{1}{z}$.

Consider the set $\mathcal{P}$ of all *positive irrational real numbers* and the set $\mathcal{N}$ of all *negative irrational real numbers* and observe that

$u(\mathcal{P}) \subset \mathcal{N}$ and $v^{\pm}(\mathcal{N}) \subset \mathcal{P}$

We have to show that no alternating word $w = (u)v^{\pm}uv^{\pm}u \dots v^{\pm}(u)$ in u and $v^{\pm}$ can be the identity in $PSL_2(\mathbb{Z})$.

If the length of w is odd then either $w(\mathcal{P}) \subset \mathcal{N}$ or $w(\mathcal{N}) \subset \mathcal{P}$ depending on whether w starts with a u or with a $v^{\pm}$ term. Either way, this proves that no odd-length word can be the identity element in $PSL_2(\mathbb{Z})$.

If the length of the word w is even we can assume that $w = v^{\pm}uv^{\pm}u \dots v^{\pm}u$ (if necessary, after conjugating with u we get to this form).

There are two subcases, either $w = v^{-1}uv^{\pm}u \dots v^{\pm}u$ in which case $w(\mathcal{P}) \subset v^{-1}(\mathcal{N})$ and this latter set is contained in the set of all positive irrational real numbers which are *strictly larger than one*.

Or, $w = vuv^{\pm}u \dots v^{\pm}u$ in which case $w(\mathcal{P}) \subset v(\mathcal{N})$ and this set is contained in the set of all positive irrational real numbers *strictly smaller than one*.

Either way, this shows that w cannot be the identity morphism on $\mathcal{P}$ so cannot be the identity element in $PSL_2(\mathbb{Z})$. Hence we have proved that

$PSL_2(\mathbb{Z}) = C_2 * C_3 = \langle u, v : u^2 = 1 = v^3 \rangle$

A description of $SL_2(\mathbb{Z})$ in terms of generators and relations follows

$SL_2(\mathbb{Z}) = \langle U, V : U^4 = 1 = V^6, U^2 = V^3 \rangle$

It is *not* true that $SL_2(\mathbb{Z})$ is the free product $C_4 * C_6$ as there is the extra relation $U^2 = V^3$.

This relation says that the cyclic groups $C_4 = \langle U \rangle$ and $C_6 = \langle V \rangle$ share a common subgroup $C_2 = \langle U^2 = V^3 \rangle$ and this extra condition is expressed by saying that $SL_2(\mathbb{Z})$ is the *amalgamated free product* of C_4 with C_6, amalgamated over the common subgroup C_2 and denoted as

$SL_2(\mathbb{Z}) = C_4 *_{C_2} C_6$

More generally, if G and H are finite groups, then the *free product* $G * H$ consists of all words of the form $(g_1)h_1g_2h_2g_3 \dots g_nh_n(g_{n-1})$ (so alternating between non-identity elements of G and H) and the group-law is induced by concatenation of words (and group-laws in either G or H when end terms are elements in the same group).

For example, take the dihedral groups $D_4 = \langle U, R : U^4 = 1 = R^2, (RU)^2 = 1\rangle$ and $D_6 = \langle V, S : V^6 = 1 = S^2, (SV)^2 = 1\rangle$ then the free product can be expressed as

$$D_4 * D_6 = \langle U, V, R, S : U^4 = 1 = V^6 = R^2 = S^2 = (RV)^2 = (RU)^2\rangle$$

This *almost* fits in with our obtained description of $GL_2(\mathbb{Z})$

$$GL_2(\mathbb{Z}) = \langle U, V, R : U^4 = 1 = V^6 = R^2 = (RU)^2 = (RV)^2, U^2 = V^3\rangle$$

except for the *extra* relations $R = S$ and $U^2 = V^3$ which express the fact that we demand that D_4 and D_6 have the same subgroup

$$D_2 = \langle U^2 = V^3, S = R\rangle$$

So, again we can express these relations by saying that $GL_2(\mathbb{Z})$ is the *amalgamated free product* of the subgroups $D_4 = \langle U, R\rangle$ and $D_6 = \langle V, R\rangle$, amalgamated over the common subgroup $D_2 = C_2 \times C_2 = \langle U^2 = V^3, R\rangle$. We write

$$GL_2(\mathbb{Z}) = D_4 *_{D_2} D_6$$

Similarly (but a bit easier) for $PGL_2(\mathbb{Z})$ we have

$$PGL_2(\mathbb{Z}) = \langle u, v, R \mid u^2 = v^3 = 1 = R^2 = (Ru)^2 = (Rv)^2\rangle$$

which can be seen as the amalgamated free product of $D_2 = \langle u, R\rangle$ with $D_3 = \langle v, R\rangle$, amalgamated over the common subgroup $C_2 = \langle R\rangle$ and therefore

$$PGL_2(\mathbb{Z}) = D_2 *_{C_2} D_3$$

Now let us turn to congruence subgroups of the modular group. With $\Gamma(n)$ one denotes the kernel of the natural surjection

$$PSL_2(\mathbb{Z}) \to PSL_2(\mathbb{Z}/n\mathbb{Z})$$

that is all elements represented by a matrix

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

such that $a = d = 1$ (mod n) and $b = c = 0$ (mod n). On the other hand $\Gamma_0(n)$ consists of elements represented by matrices such that only $c = 0$ (mod n). Both are finite index subgroups of $PSL_2(\mathbb{Z})$.

As we have seen that $PSL_2(\mathbb{Z}) = C_2 * C_3$ it follows from general facts on free products that any finite index subgroup is of the form

$$C_2 * C_2 * \cdots * C_2 * C_3 * C_3 * \cdots * C_3 * C_\infty * C_\infty \cdots * C_\infty$$

that is the free product of k copies of C_2, l copies of C_3 and m copies of C_∞ where it should be noted that k,l and m are allowed to be zero. There is an elegant way to calculate explicit generators of these factors for congruence subgroups, due to Ravi S. Kulkarni (An Arithmetic-Geometric Method in the Study of the Subgroups of the Modular Group , American Journal of Mathematics, Vol. 113, No. 6. (Dec., 1991), pp. 1053-1133) which we will discuss later.

Using this method one finds that $\Gamma_0(2)$ is generated by the Moebius transformations corresponding to the matrices

$$X = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } Y = \begin{bmatrix} 1 & -1 \\ 2 & -1 \end{bmatrix}$$

and that generators for $\Gamma(2)$ are given by the matrices

$$A = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 1 & -2 \\ 2 & -3 \end{bmatrix}$$

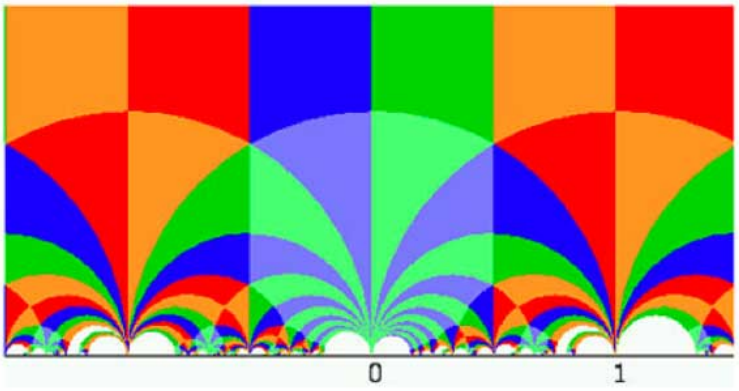
Next, one has to write these generators in terms of the generating matrices u and v of $PSL_2(\mathbb{Z})$ and as we know all relations between u and v the relations of these congruence subgroups will follow.

We will give the details for $\Gamma_0(2)$ and leave you to figure out that $\Gamma(2) = C_\infty * C_\infty$ (that is that there are no relations between the matrices A and B).

Calculate that $X = v^2u$ and that $Y = vuv^2$. Because the only relations between u and v are $v^3 = 1 = u^2$ we see that Y is an element of order two as $Y^2 = vuv^3uv^2 = v^3 = 1$ and that no power of X can be the identity transformation.

But then also none of the elements $(Y)X^{i_1}YX^{i_2}Y\ldots YX^{i_n}(Y)$ can be the identity (write it out as a word in u and v) whence, indeed

$\Gamma_0(2) = C_\infty * C_2$



The picture is due to Helena Verrill and she has a page with more pictures. The picture above depicts a way to get a fundamental domain for the action of $\Gamma_0(2)$ on the upper half plane. Such a fundamental domain consists of any choice of 6 tiles with different colours (note that there are two shades of blue and green). Helena also has a Java-applet to draw fundamental domains of more congruence subgroups.

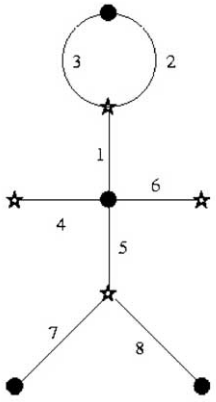
2.8 Permutation representations of monodromy groups

We will explain how curves defined over $\overline{\mathbb{Q}}$ determine permutation representations of the *carthographic groups*.

We have seen that any smooth projective curve C (a Riemann surface) defined over the algebraic closure $\overline{\mathbb{Q}}$ of the rationals, defines a *Belyi map* $C \xrightarrow{\pi} \mathbb{P}^1$ which is only ramified over the three points
$0, 1, \infty$.

By this we mean that there are exactly d points of C lying over any other point of $\mathbb{P}^1$ (we call d the degree of π) and that the number of points over $0, 1$ and ∞ is smaller than d. To such a map we associate a *dessin dénfant*, a drawing on C linking the pre-images of 0 and 1 with exactly d edges (the preimages of the open unit-interval).

Next, we look at the preimages of 0 and associate a permutation τ_0 of d letters to it by cycling counter-clockwise around these preimages and recording the edges we meet. We repeat this procedure for the preimages of 1 and get another permutation τ_1. That is, we obtain a subgroup of the symmetric group $\langle \tau_0, \tau_1 \rangle \subset S_d$ which is called the *monodromy group* of the covering π.

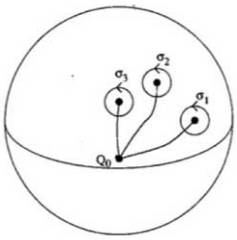


For example, the dessin on the leftis associated to a degree 8 map $\mathbb{P}^1 \to \mathbb{P}^1$ and if we let the black (resp. starred) vertices be the preimages of 0 (respectively of 1), then the corresponding partitions are $\tau_0 = (2,3)(1,4,5,6)$ and $\tau_1 = (1,2,3)(5,7,8)$ and the monodromy group is the alternating group A_8 (use GAP).

But wait! The map is also ramified in ∞ so why donť we record also a permutation τ_∞ and are able to compute it from the dessin? (Note that all three partitions are needed if we want to reconstruct C from the d sheets as they encode in which order the sheets fit together around the preimages).

Well, the monodromy group of a $\mathbb{P}^1$ covering ramified only in three points is an epimorphic image of the fundamental group of the sphere minus three points $\pi_1(\mathbb{P}^1 - 0, 1, \infty)$. That is, the group of all loops beginning and ending in a basepoint upto homotopy (that is, two such loops are the same if they can be transformed into each other in a continuous way while avoiding the three points).

This group is generated by loops σ_i running from the basepoint to nearby the i-th point, doing a counter-clockwise walk around it and going back to be basepoint Q_0 and the epimorphism to the monodromy group is given by sending

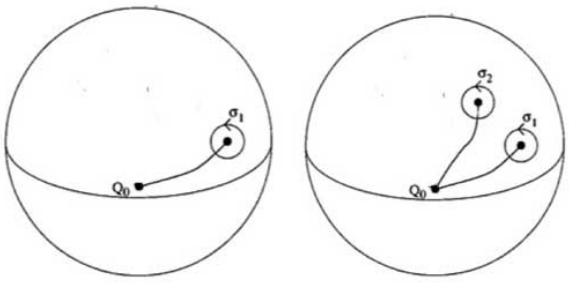


$$\sigma_1 \mapsto \tau_0 \qquad \sigma_2 \mapsto \tau_1 \qquad \sigma_3 \mapsto \tau_\infty$$

Now, these three generators are not independent. In fact, this fundamental group is

$$\pi_1(\mathbb{P}^1 - \{0,1,\infty\}) = \langle \sigma_1, \sigma_2, \sigma_3 \mid \sigma_1\sigma_2\sigma_3 = 1 \rangle$$

To understand this, let us begin with an easier case, that of the sphere minus one point. The fundamental group of the plane minus one point is $\mathbb{Z}$ as it encodes how many times we walk around the point. However, on the sphere the situation is different as we can make our walk around the point longer and longer until the whole walk is done at the backside of the sphere and then we can just contract our walk to the base point. So, there is just one type of walk on a sphere minus one point (up to homotopy) whence this fundamental group is trivial. Next, let us consider the sphere minus two points

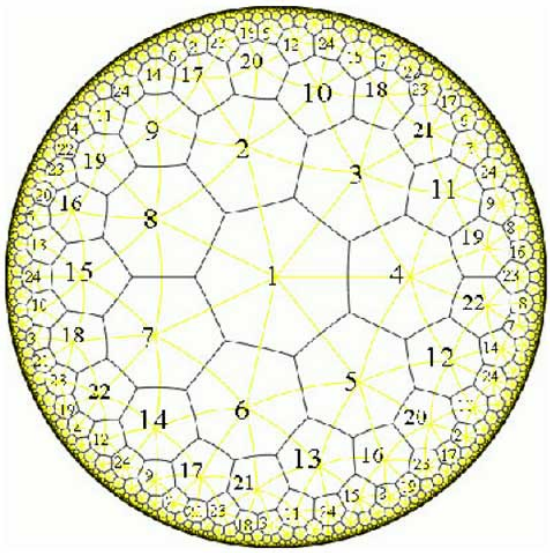


Repeat the foregoing to the walk σ_2, that is, strech the upper part of the circular tour all over the backside of the sphere and then we see that we can move it to fit with the walk σ_1 BUT for the orientation of the walk! That is, if we do this modified walk $\sigma_1\sigma_2^{'}$ we just made the trivial walk. So, this fundamental group is $\langle \sigma_1, \sigma_2 \mid \sigma_1\sigma_2 = 1 \rangle = \mathbb{Z}$ This is also the proof of the above claim. For, we can modify the third walk σ_3 continuously so that it becomes the walk $\sigma_1\sigma_2$ but with the *reversed orientation*!

As $\sigma_3 = (\sigma_1\sigma_2)^{-1}$ this allows us to compute the ḿissingṕermutation $\tau_\infty = (\tau_0\tau_1)^{-1}$ In the example above, we obtain $\tau_\infty = (1,2,6,5,8,7,4)(3)$ so it has two cycles corresponding to the fact that the dessin has two regions (remember we should draw ths on the sphere) : the head and the outer-region. Hence, the pre-images of ∞ correspond to the different regions of the dessin on the curve C. For another example, consider the degree 168 map

$K \to \mathbb{P}^1$

which is the modified orbit map for the action of $PSL_2(\mathbb{F}_7)$ on the Klein quartic. The corresponding dessin is the heptagonal construction of the Klein quartic



Here, the pre-images of 1 correspond to the midpoints of the 84 edges of the polytope whereas the pre-images of 0 correspond to the 56 vertices. We can label the 168 half-edges by numbers such that τ_0 and τ_1 are the standard generators b resp. a of the 168-dimensional regular representation (see the atlas page).

Calculating with GAP the element $\tau_\infty = (\tau_0\tau_1)^{-1} = (ba)^{-1}$ one finds that this permutation consists of 24 cycles of length 7, so again, the pre-images of ∞ lie one in each of the 24 heptagonal regions of the Klein quartic. Now, we are in a position to relate curves defined over $\overline{Q}$ via their Belyi-maps and corresponding dessins to Grothendiecks carthographic groups $\Gamma(2)$, $\Gamma_0(2)$ and $SL_2(\mathbb{Z})$.

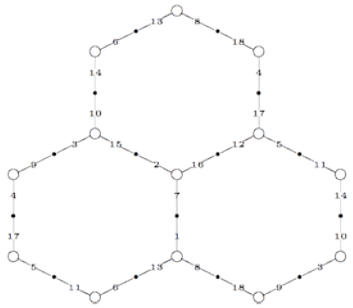
The dessin gives a permutation representation of the monodromy group and because the fundamental group of the sphere minus three points $\pi_1(\mathbb{P}^1 - 0,1,\infty) = \langle \sigma_1, \sigma_2, \sigma_3 \mid \sigma_1\sigma_2\sigma_3 = 1 \rangle = \langle \sigma_1, \sigma_2 \rangle$ is the free group op two generators, we see that any dessin determines a permutation representation of the congruence subgroup $\Gamma(2)$.

A **clean dessin** is one for which one type of vertex has all its valancies (the number of edges in the dessin meeting the vertex) equal to one or two. (for example, the pre-images of 1 in the Klein quartic-dessin or the pre-images of 1 in the *monsieur Mathieu example*).

The corresponding permutation τ_1 then consists of 2-cycles and hence the monodromy group gives a permutation representation of the free product $C_\infty * C_2 = \Gamma_0(2)$ Finally, a clean dessin is said to be a *quilt dessin* if also the other type of vertex has all its valancies equal to one or three (as in the Klein quartic or Mathieu examples).

Then, the corresponding permutation has order 3 and for these quilt-dessins the monodromy group gives a permutation representation of the free product $C_2 * C_3 = PSL_2(\mathbb{Z})$.

2.9 Modular quilts and cuboid tree diagrams



Conjugacy classes of finite index subgroups of the modular group $\Gamma = PSL_2(\mathbb{Z})$ are determined by a combinatorial gadget : a *modular quilt*.

By this we mean a finite connected graph drawn on a Riemann surface such that its vertices are either black or white. Moreover, every edge in the graph connects a black to a white vertex and the valency (that is, the number of edges incident to a vertex) of a black vertex is either 1 or 2, that of a white vertex is either 1 or 3. Finally, for every white vertex of valency 3, there is a prescribed cyclic order on the edges incident to it.

On the left a modular quilt consisting of 18 numbered edges (some vertices and edges re-appear) which gives a honeycomb tiling on a torus. All white vertices have valency 3 and the order of the edges is given by walking around a point in counterclockwise direction. For example, the order of the edges at the top left vertex (which re-appears at the middle right vertex) can be represented by the 3-cycle (6,11,14), that around the central vertex gives the 3-cycle (2,7,16).

We have seen that the modular group Γ is freely generated by the two elements

$$U = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad V = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$$

and remark that $U^2 = V^3 = 1$. To a modular quilt having d edges we can associate a transitive permutation representation of Γ on d letters (the labels of the edges) such that the action of U is given by the order two permutation given by the product of all 2-cycles of incident edges to black 2-valent vertices and the action of V is given by the order three permutation given by the cyclic ordering of edges around white 3-valent vertices in the quilt. For the example above we have

$U \to (1,7)(2,15)(3,9)(4,17)(5,11)(6,13)(8,18)(10,14)(12,16)$

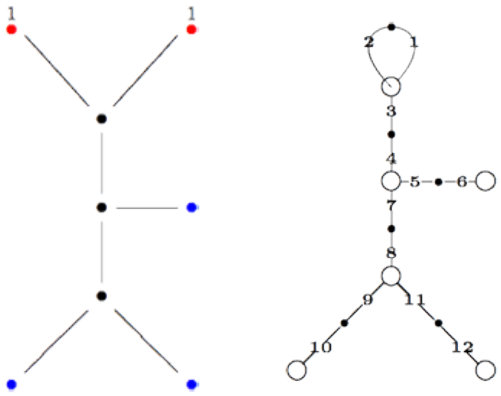
$V \to (1,13,8)(2,7,16)(3,15,10)(4,9,18)(5,17,12)(6,11,14)$

The (index d) subgroup of Γ corresponding to the modular quilt is then the stabilizer subgroup of a fixed edge. Note that choosing a different edge gives a conjugate subgroup.

Conversely, given an index d subgroup G we can label the d left-cosets in Γ/G by the numbers 1,2,...,d and describe the action of left multiplication by U and V on the cosets as permutations in the symmetric group S_d. Because U has order two, its permutation will be a product of two cycles which we can interprete as giving the information on edges incident to 2-valent black vertices. Similarly, V has order three and hence its permutation consists of 3-cycles giving the ordering of edges around 3-valent white vertices. Edges not appearing in U (resp. V) have as their leaf-vertex a black (resp. white) vertex of valency 1. Because the permutation action is transitive, this procedure gives a connected graph on d edges, d white and d black vertices and is a modular quilt.

In order to connect modular quilts to *special hyperbolic polygons* we need the intermediate concept of *cuboid tree diagrams*. These are trees (that is, connected graphs without cycles)

such that all internal vertices are 3-valent (and have an order on the incident edges) and the leaf-vertices are tinted either red or blue. In addition, there is an involution on the red vertices.



The tree on the left is a cuboid tree, the involution interchanges the two top red vertices (indicated by having the same number). We associate to such a cuboid tree diagram a modular quilt by taking as the white vertices : all internal vertices together with the blue leaf-vertices, and as the black vertices : the midpoints of internal edges, together with the midpoints of edges connecting a blue leaf-vertex, together will all red leaf-vertices. If two red leaf-vertices correspond under the involution, we glue the corresponding black vertices together.

That is, the picture of the right is the resulting modular quilt. Conversely, starting with a modular quilt we can always construct from it a cuboid tree diagram by breaking cycles in black vertices until there are no cycles left. All black leaf-vertices in the resulting tree are tinted red and correspond under the involution when they came from the same black quilt-vertex. Remaining leaf-vertices are tinted blue. All internal black vertices are removed (and the edges incident to them glued into larger edges) and all internal white vertices become the internal vertices of the cuboid tree.

While a cuboid tree diagram determines the modular quilt uniquely, there are in general several choices of breaking up cycles in a modular quilt, so also several cuboid tree diagrams determining the same modular quilt. That is, we have shown that there are natural maps

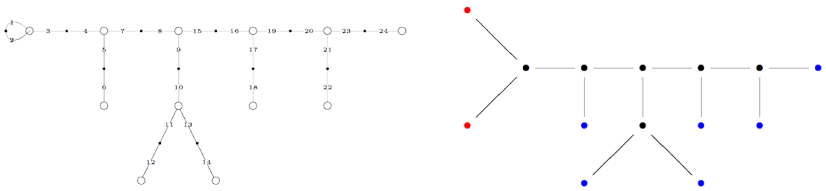
cuboid tree $\longrightarrow\!\!\!\!\!\rightarrow$ modular quilt $\leftrightarrow$ conjugacy class of finite index subgroup

where the first map is finite to one and the second map is a bijection.

Observe that we can also use modular quilts (or their associated cuboid trees) as a mnemotechnic device to remember the construction of groups, generated by an order two and an order three element and having a low dimensional faithful permutation representation. For example, the sporadic simple Mathieu group M_{12} has a 12-dimensional permutation representation encoded by the above left quilt, which we call the M_{12} *quilt*. That is, M_{12} is generated by the two permutations

(1,2)(3,4)(5,6)(7,8)(9,10)(11,12) and (1,2,3)(4,7,5)(8,9,11)

Hence the cuboid tree on the right can be called the M_{12} *tree*. Similarly, the sporadic simple Mathieu group M_{24} has a 24-dimensional permutation representation which can be represented by the modular quilt, the M_{24} *quilt*



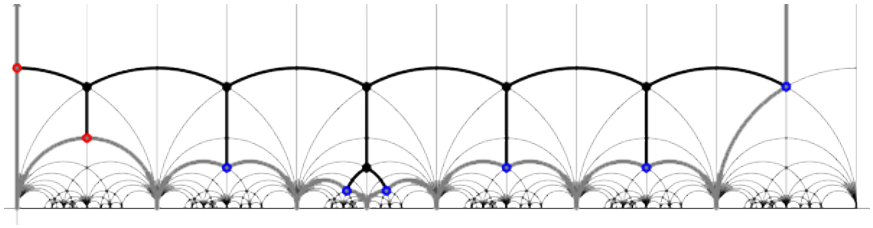
That is, M_{24} is generated by the permutations (1,2,3)(4,5,7)(8,9,15)(10,11,13)(16,17,19)(20,21,23) and (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)(13,14)(15,16)(17,18)(19,20)(21,22)(23,24) with corresponding M_{24} *tree* with the two red vertices interchanging under the involution.

References :

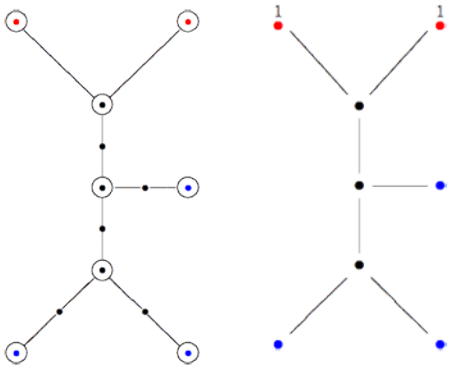
Tim Hsu, "Permutation techniques for cosed representations of modular subgroups"

Ravi S. Kulkarni, "An arithmetic-geometric method in the study of the subgroups of the modular group" Amer. J. Math. 113 (1991) 1053-1133

2.10 Hyperbolic Mathieu polygons



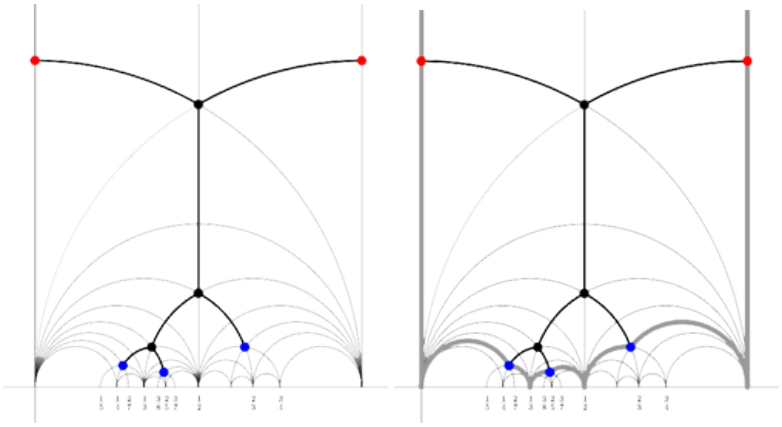
We will link *modular quilts* (via their associated cuboid tree diagrams) to *special hyperbolic polygons*. The above drawing gives the hyperbolic polygon (the gray boundary) associated to the M_{24} tree diagram (the black interior graph). In general, the correspondence goes as follows.



Recall that a cuboid tree diagram is a tree such that all internal vertices are 3-valent and have a specified ordering on the incident edges (given by walking counterclockwise around the vertex) and such that all leaf-vertices are tinted blue or red, the latter ones are paired via an involution (indicated by giving paired red vertices the same label). Introduce a new

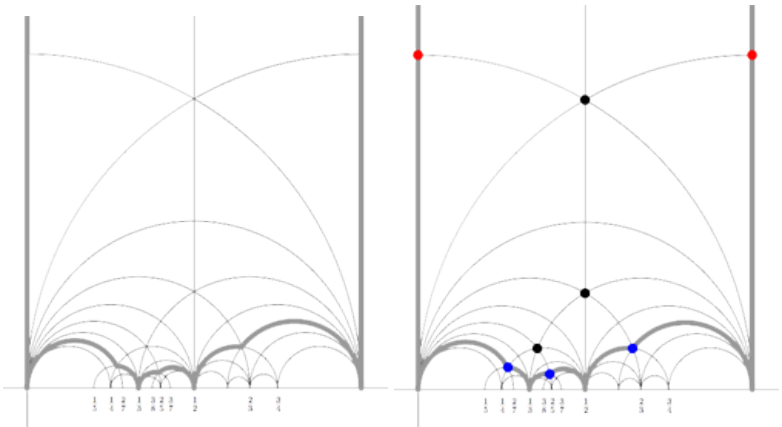
2-valent vertex on all edges joining two internal vertices or a blue vertex to an internal vertex.

So, the picture on the right corresponds to the tree diagram on the left. Equip this extended tree with a metric such that every edge has length equal to an f-edge in the *Dedekind tessellation*. Fix an edge having a red vertex and develop this isometrically onto the f-edge connecting i to ρ in the tessellation. Then, the extended tree develops uniquely along the f-edges of the tessellation and such that the circled black and blue vertices correspond to odd vertices, the circled red and added uncircled vertices correspond to even vertices in the tessellation. Starting from the above tree (and choosing the upper-left edge to start the embedding), we obtain the picture on the left (we have removed the added 2-valent vertices)



We will now associate a *special hyperbolic polygon* to this tree. At a red vertex take the even line going through the vertex. If under the involution the red vertex is send to itself, the even edges will be paired.

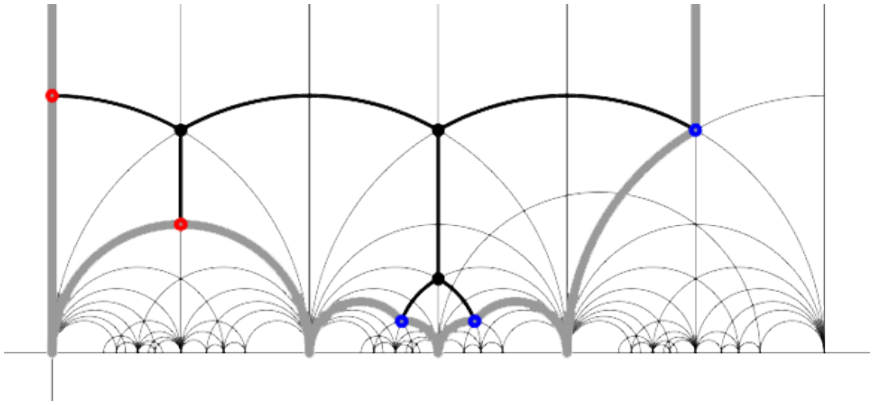
Otherwise, the line is a free side and will be paired to the free side containing the red vertex corresponding under the involution. At a blue vertex, take the two odd edges making an angle of $\frac{\pi}{3}$ with the tree-edge containing the blue vertex. These odd edges will be paired. If we do this procedure for all blue and red vertices, we obtain a special polygon (see the picture on the right, the two vertical lines are paired). Conversely, suppose we start with a special polygon such as the one on the left below



and consider all even and odd vertices on the boundary (which are tinted red, respectively blue) together with all odd vertices in the interior of the special polygon. These are indi-

cated in the picture on the right above. If we connect these vertices with the geodesics in the polygon we get a cuboid tree diagram.

This correspondence special polygons $\longrightarrow\!\!\!\!\!\rightarrow$ tree diagrams is finite to one as we have made a choice in the starting red vertex and edge. If we would have taken the other edge containing a red vertex we would end up with the following special polygon



It is no accident that these two special polygons consist of exactly 24 triangles of the Dedekind tessellation as they correspond to the index 12 subgroup of the modular group Γ determining the 12-dimensional permutation representation of the Mathieu group M_{12}. Similarly, the top drawing has 48 hyperbolic triangles and corresponds to the 24-dimensional permutation representation of M_{24}. Next time, we will make the connection with *Farey series* which will allow us to give free generators of finite index subgroups.

Reference :

Ravi S. Kulkarni, "An arithmetic-geometric method in the study of the subgroups of the modular group", Amer. J. Math. 113 (1991) 1053-1133

2.11 Farey codes

John Farey (1766-1826) was a geologist of sorts. Eyles, quoted on the math-biographies site described his geological work as

"As a geologist Farey is entitled to respect for the work which he carried out himself, although it has scarcely been noticed in the standard histories of geology."

That we still remember his name after 200 years is due to a short letter he wrote in 1816 to the editor of the Philosophical Magazine

"On a curious Property of vulgar Fractions. By Mr. J. Farey, Sen. To Mr. Tilloch

Sir. - On examining lately, some very curious and elaborate Tables of "Complete decimal Quotients," calculated by Henry Goodwyn, Esq. of Blackheath, of which he has printed a copious specimen, for private circulation among curious and practical calculators, preparatory to the printing of the whole of these useful Tables, if sufficient encouragement, either public or individual, should appear to warrant such a step: I was fortunate while so doing, to deduce from them the following general property; viz.

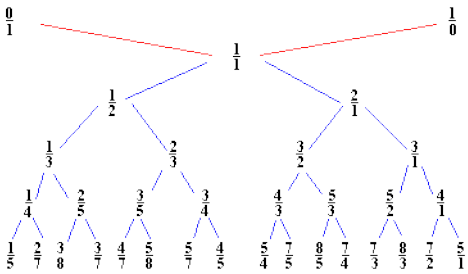
If all the possible vulgar fractions of different values, whose greatest denominator (when in their lowest terms) does not exceed any given number, be arranged in the order of their values, or quotients; then if both the numerator and the denominator of any fraction therein,

be added to the numerator and the denominator, respectively, of the fraction next but one to it (on either side), the sums will give the fraction next to it; although, perhaps, not in its lowest terms.

For example, if 5 be the greatest denominator given; then are all the possible fractions, when arranged, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, and 4/5; taking 1/3, as the given fraction, we have (1+1)/(5+3) = 2/8 = 1/4 the next smaller fraction than 1/3; or (1+1)/(3+2) = 2/5, the next larger fraction to 1/3. Again, if 99 be the largest denominator, then, in a part of the arranged Table, we should have 15/52, 28/97, 13/45, 24/83, 11/38, and if the third of these fractions be given, we have (15+13)/(52+45) = 28/97 the second: or (13+11)/(45+38) = 24/83 the fourth of them: and so in all the other cases.

I am not acquainted, whether this curious property of vulgar fractions has been before pointed out?; or whether it may admit of any easy or general demonstration?; which are points on which I should be glad to learn the sentiments of some of your mathematical readers; and am

Sir, Your obedient humble servant, J. Farey. Howland-street."



So, if we interpolate "childish addition of fractions" $\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}$ and start with the numbers $0 = \frac{0}{1}$ and $\infty = \frac{1}{0}$ we get the binary Farey-tree. For a fixed natural number n, if we stop the interpolation whenever the denominator of the fraction would become larger than n and order the obtained fractions (smaller or equal to one) we get the Farey sequence F(n). For example, if n=3 we start with the sequence $\frac{0}{1}, \frac{1}{1}$. The next step we get $\frac{0}{1}, \frac{1}{2}, \frac{1}{1}$ and the next step gives

$$\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}$$

and as all the denomnators of childish addition on two consecutive fractions will be larger than 3, the above sequence is F(3). A remarkable feature of the series F(n) is that if $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive terms in F(n), then

$$det \begin{bmatrix} a & c \\ b & d \end{bmatrix} = -1$$

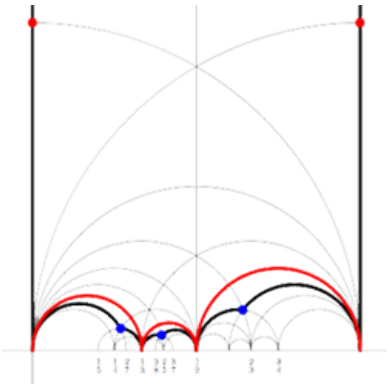
and so these two fractions are the endpoints of an even geodesic in the *Dedekind tessellation*.

A *generalized Farey series* is an ordered collection of fractions $\infty, x_0, x_1, \cdots, x_n, \infty$ such that x_0 and x_n are integers and some $x_i = 0$. Moreover, writing $x_i = \frac{a_i}{b_i}$ we have that

$$det \begin{bmatrix} a_i & a_{i+1} \\ b_i & b_{i+1} \end{bmatrix} = -1$$

A *Farey code* is a generalized Farey sequence consisting of all the vertices of a *special polygon* that lie in $\mathbb{R} \cup \{\infty\}$ together with side-pairing information. If two consecutive terms are such that the complete geodesic between x_i and x_{i+1} consists of two sides of the polygon which are paired we denote this fact by $x_i \overset{}{\underset{\circ}{\text{———}}} x_{i+1}$.

If they are the endpoints of two odd sides of the polygon which are paired we denote this by $x_i \overset{}{\underset{\bullet}{\text{———}}} x_{i+1}$. Finally, if they are the endpoints of a free side which is paired to another free side determined by x_j and x_{j+1} we denote this fact by marking both edges $x_i \overset{}{\underset{k}{\text{———}}} x_{i+1}$ and $x_j \overset{}{\underset{k}{\text{———}}} x_{j+1}$ with the same number.



For example, for the M_{12} special polygon on the left (bounded by the thick black geodesics), the only vertices in $\mathbb{R} \cup \{\infty\}$ are $\infty, 0, \frac{1}{3}, \frac{1}{2}, 1$. The two vertical lines are free sides and are paired, whereas all other sides of the polygon are odd. Therefore the Farey-code for this Mathieu polygon is

$$\infty \underset{1}{\text{———}} 0 \underset{\bullet}{\text{———}} \frac{1}{3} \underset{\bullet}{\text{———}} \frac{1}{2} \underset{\bullet}{\text{———}} 1 \underset{1}{\text{———}} \infty$$

Conversely, to a Farey-code we can associate a special polygon by first taking the hyperbolic convex hull of all the terms in the sequence (the region bounded by the vertical lines and the bottom red circles in the picture on the left) and adding to it for each odd interval $x_i \underset{\bullet}{\text{———}} x_{i+1}$ the triangle just outside the convex hull consisting of two odd edges in the Dedekind tessellation (then we obtain the region bounded by the black geodesics). Again, the side-pairing of the obained special polygon can be obtained from that of the Farey-code. This correspondence gives a natural one-to-one correspondence

special polygons $\leftrightarrow$ Farey-codes

Later we will see how the Farey-code determines the group structure of the corresponding finite index subgroup of the modular group $\Gamma = PSL_2(\mathbb{Z})$.

Reference :

Ravi S. Kulkarni, "An arithmetic-geometric method in the study of the subgroups of the modular group", Amer. J. Math 113 (1991) 1053-1133

2.12 Generators of modular subgroups

Wehave already seen that the modular group $\Gamma = PSL_2(\mathbb{Z})$ is the group free product $C_2 * C_3$, so let's just skim over details here. First one observes that Γ is generated by (the images of) the invertible 2x2 matrices

$$U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ and } V = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$$

A way to see this is to consider X=U.V and Y=V.U and notice that multiplying with powers of X adds multiples of the second row to the first (multiply on the left) or multiples of the first column to the second (multiply on the right) and the other cases are handled by taking multiples with powers of Y. Use this together with the fact that matrices in $GL_2(\mathbb{Z})$ have their rows and columns made of coprime numbers to get any such matrix by multiplication on the left or right by powers of X and Y into the form

$$\begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix} \text{ and because } U^2 = V^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

we see that Γ is an epimorphic image of $C_2 * C_3$. To prove isomorphism one can use the elegant argument due to Roger Alperin considering the action of the Moebius transformations $u(z) = -\frac{1}{z}$ and $v(z) = \frac{1}{1-z}$ (with $v^{-1}(z) = 1 - \frac{1}{z}$) induced by the generators U and V on the sets $\mathcal{P}$ and $\mathcal{N}$ of all positive (resp. negative) irrational real numbers. Observe that

$u(\mathcal{P}) \subset \mathcal{N}$ and $v^{\pm}(\mathcal{N}) \subset \mathcal{P}$

Hence, if w is a word in u and $v^{\pm}$ of off length we either have $w(\mathcal{P}) \subset \mathcal{N}$ or $w(\mathcal{N}) \subset \mathcal{P}$ so w can never be the identity. If the length is even we can conjugate w such that it starts with $v^{\pm}$. If it starts with v then $w(\mathcal{P}) \subset v(\mathcal{N})$ is a subset of positive rationals less than 1 whereas if it starts with v^{-1} then $w(\mathcal{P}) \subset v^{-1}(\mathcal{N})$ is a subset of positive rationals greater than 1, so again it cannot be the identity. Done!

By a result of Aleksandr Kurosh it follows that every modular subgroup is the group free product op copies of C_2, C_3 or C_∞ and we would like to determine the free generators explicitly for a cofinite subgroup starting from its associated *Farey code* associated to a *special polygon* corresponding to the subgroup.

To every even interval $x_i = \frac{a_i}{b_i} \overset{\circ}{\text{———}} x_{i+1} = \frac{a_{i+1}}{b_{i+1}}$ in the Farey code one associates the generator of a C_2 component

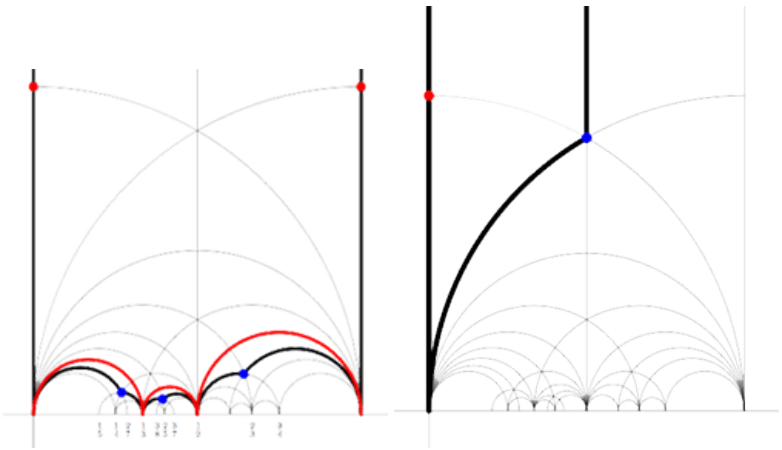
$$A_i = \begin{bmatrix} a_{i+1}b_{i+1} + a_i b_i & -a_i^2 - a_{i+1}^2 \\ b_i^2 + b_{i+1}^2 & -a_{i+1}b_{i+1} - a_i b_i \end{bmatrix}$$

to every odd interval $x_i = \frac{a_i}{b_i} \overset{\bullet}{\text{———}} x_{i+1} = \frac{a_{i+1}}{b_{i+1}}$ in the Farey code we associate the generator of a C_3 component the matrix B_i

$$\begin{bmatrix} a_{i+1}b_{i+1} + a_i b_{i+1} + a_i b_i & -a_i^2 - a_i a_{i+1} - a_{i+1}^2 \\ b_i^2 + b_i b_{i+1} + b_{i+1}^2 & -a_{i+1}b_{i+1} - a_{i+1}b_i - a_i b_i \end{bmatrix}$$

and finally, to every pair of free intervals $x_k \overset{a}{\text{———}} x_{k+1} \ \ldots \ x_l \overset{a}{\text{———}} x_{l+1}$ we associate the generator of a C_∞ component

$$C_{k,l} = \begin{bmatrix} a_l & -a_{l+1} \\ b_l & -b_{l+1} \end{bmatrix} \begin{bmatrix} a_{k+1} & a_k \\ b_{k+1} & b_k \end{bmatrix}^{-1}$$



Kulkarni's result states that these matrices are free generators of the cofinite modular subgroup determined by the Farey code. For example, for the M_{12} special polygon on the left (bounded by the thick black geodesics), the Farey-code for this Mathieu polygon is

$$\infty \overset{}{\underset{1}{\text{———}}} 0 \overset{}{\underset{\bullet}{\text{———}}} \frac{1}{3} \overset{}{\underset{\bullet}{\text{———}}} \frac{1}{2} \overset{}{\underset{\bullet}{\text{———}}} 1 \overset{}{\underset{1}{\text{———}}} \infty$$

Therefore, the structure of the subgroup must be $C_\infty * C_3 * C_3 * C_3$ with the generator of the infinite factor being

$\begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}$ and those of the cyclic factors of order three

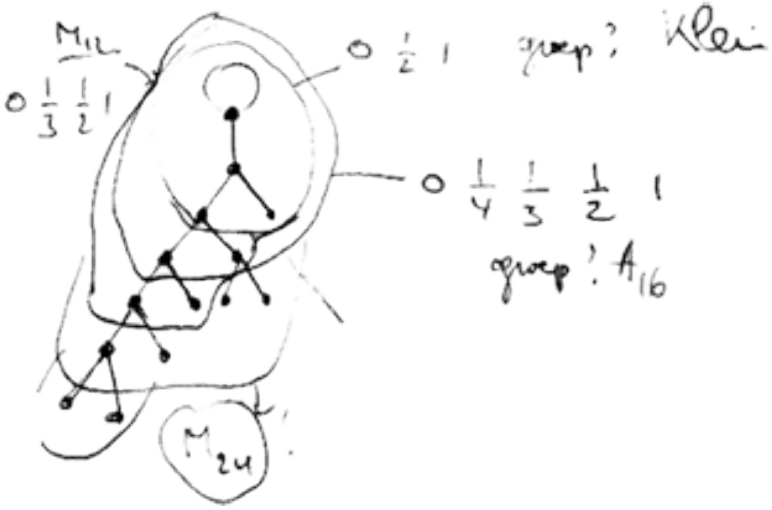
$\begin{bmatrix} 3 & -1 \\ 13 & -4 \end{bmatrix}$, $\begin{bmatrix} 7 & -3 \\ 19 & 8 \end{bmatrix}$ and $\begin{bmatrix} 4 & -3 \\ 7 & -5 \end{bmatrix}$

This approach also gives another proof of the fact that $\Gamma = C_2 * C_3$ because the Farey code to the subgroup of index 1 is $\infty \overset{}{\underset{\circ}{\text{———}}} 0 \overset{}{\underset{\bullet}{\text{———}}} \infty$ corresponding to the fundamental domain on the left. This finishes (for now) this thread on Kulkarni's paper (or rather, part of it).

Reference :

Ravi S. Kulkarni, "An arithmetic-geometric method in the study of the subgroups of the modular group", Amer. J. Math 113 (1991) 1053-1133

2.13 Iguanodon series of simple groups



Bruce Westbury has a page on recent work on series of Lie groups including exceptional groups. Moreover, he did put his slides of a recent talk (probably at MPI) online.

Probably, someone considered a similar problem for simple groups. Are there natural constructions leading to a series of finite simple groups including some sporadic groups as special members? In particular, does the following sequence appear somewhere ?

$L_2(7), M_{12}, A_{16}, M_{24}, A_{28}, A_{40}, A_{48}, A_{60}, \ldots$

Here, $L_2(7)$ is the simple group of order 168 (the automorphism group of the Klein quartic), M_{12} and M_{24} are the sporadic Mathieu groups and the A_n are the alternating simple groups.

I've stumbled upon this series playing around with Farey sequences and their associated 'dessins d'enfants' (I'll come back to the details of the construction in the second part) and have dubbed this sequence the *Iguanodon* series because the shape of the doodles leading to its first few terms

reminded me of the Iguanodons of Bernissart (btw. this sketch outlines the construction to the experts). *Conjecturally*, all groups appearing in this sequence are simple and probably all of them (except for the first few) will be alternating.

I did verify that none of the known low-dimensional permutation representations of other sporadic groups appear in the series. However, there are plenty of similar sequences one can construct from the Farey sequences, and it would be nice if one of them would contain the Conway group Co_1. (to be continued)

2.14 The iguanodon disected

Here the details of the *iguanodon series*. Start with the Farey sequence $F(n)$ of order n which is the sequence of completely reduced fractions between 0 and 1 which, when in lowest terms, have denominators less than or equal to n, arranged in order of increasing size. Here are the first eight Fareys

$F(1) = \{\frac{0}{1}, \frac{1}{1}\}$

$F(2) = \{\frac{0}{1}, \frac{1}{2}, \frac{1}{1}\}$

$F(3) = \{\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}\}$

$F(4) = \{\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}\}$

$F(5) = \{\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\}$

$F(6) = \{\frac{0}{1}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{1}{1}\}$

$F(7) = \{\frac{0}{1}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \frac{1}{1}\}$

$F(8) = \{\frac{0}{1}, \frac{1}{8}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{3}{8}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{5}{8}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \frac{7}{8}, \frac{1}{1}\}$

Fig. 2.5: Edmund Landau

Farey sequences have plenty of mysterious properties. For example, in 1924 J. Franel and Edmund Landau proved that an asymptotic density result about Farey sequences is equivalent to the Riemann hypothesis. More precisely, let a(n) be the number of terms in the Farey sequence F(n) (that is, a(1)=2,a(2)=3,...,a(8)=23 etc). This is sequence A005728 in the online integer sequences catalog. Let $F(n)_j$ denote the j-th term in F(n), then the following conjecture is equivalent to the Riemann hypothesis

For every $\epsilon > 0$ there is a constant C depending on ϵ such that

$$\sum_{j=1}^{a(n)} |F(n)_j - \frac{j}{a(n)}| < Cn^{\frac{1}{2}+\epsilon}$$

when n goes to infinity. Anyway, let us continue our construction.

Farey sequences are clearly symmetric around $\frac{1}{2}$ so let us just take half of them, so we jump to 1 when we have reached $\frac{1}{2}$. Let us extend this halved Farey on both sides with ∞ and call it the *modified Farey sequence* $f(n)$. For example,

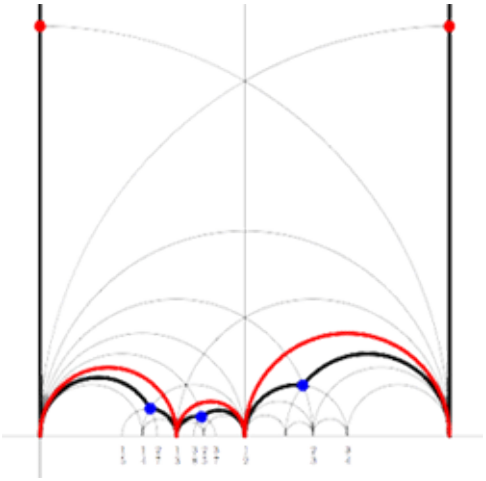
$f(3) = \{\infty, 0, \frac{1}{3}, \frac{1}{2}, 1, \infty\}$

Now consider the *Farey code* (see the second part) in which we identify the two sides connected to ∞ and mark two consecutive Farey numbers as

$$f(n)_i \overset{}{\underset{\bullet}{\text{———}}} f(n)_{i+1}$$

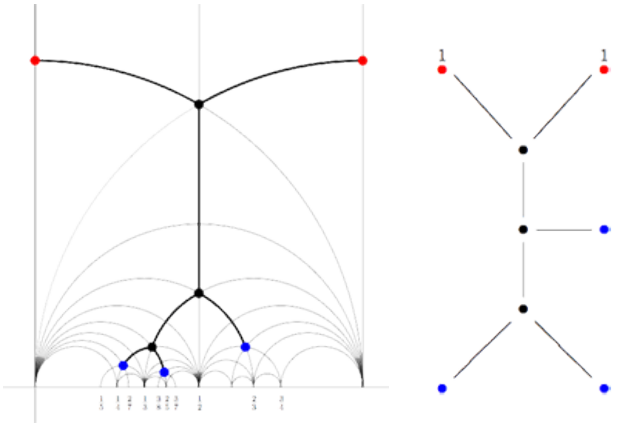
That is, the Farey code associated to the modified sequence $f(3)$ is

$$\infty \overset{}{\underset{1}{\text{———}}} 0 \overset{}{\underset{\bullet}{\text{———}}} \frac{1}{3} \overset{}{\underset{\bullet}{\text{———}}} \frac{1}{2} \overset{}{\underset{\bullet}{\text{———}}} 1 \overset{}{\underset{1}{\text{———}}} \infty$$



In the second part we will see that to a Farey-code we can associate a special polygon by first taking the hyperbolic convex hull of all the terms in the sequence (the region bounded by the vertical lines and the bottom red circles in the picture on the left) and adding to it for each odd interval $f(n)_i \overset{}{\underset{\bullet}{\text{———}}} f(n)_{i+1}$ the triangle just outside the convex hull consisting of two odd edges in the Dedekind tessellation (then we obtain the region bounded by the black geodesics for the sequence $f(3)$).

Next, we can associate to this special polygon a *cuboid tree diagram* (see also the second part) by considering all even and odd vertices on the boundary (which are tinted red, respectively blue) together with all odd vertices in the interior of the special polygon. These are indicated in the left picture below. If we connect these vertices with the geodesics in the polygon we get a cuboid tree diagram. The obtained cuboid tree diagram is depicted on the right below.



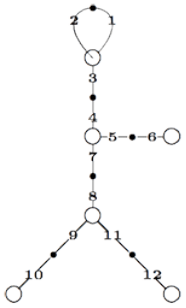
Finally, identifying the red points (as they lie on geodesics connected to ∞ which are identified in the Farey code), adding even points on the remaining geodesics and numbering the obtained half-lines we obtain the dessin d'enfant given on the left hand side.

To such a dessin we can associate its monodromy group which is a permutation group on the half-lines generated by an order two element indicating which half-lines make up a line and an order three element indicating which half-lines one encounters by walking counter-clockwise around a three-valent vertex. For the dessin on the left the group is therefore the subgroup of S_{12} generated by the elements

$\alpha = (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)$

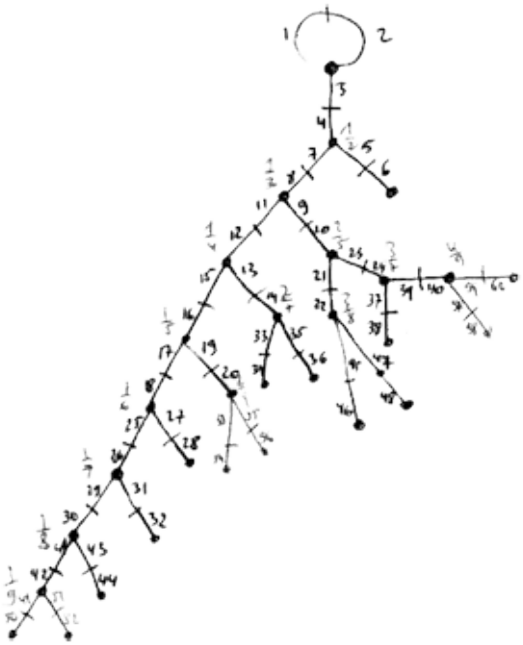
$\beta = (1,2,3)(4,5,7)(8,9,11)$

and a verification with GAP tells us that this group is the sporadic Mathieu group M_{12}. This concludes the description of the second member of the Iguanodon series. If you like to check that the first 8 iguanodons are indeed the simple groups



$L_2(7), M_{12}, A_{16}, M_{24}, A_{28}, A_{40}, A_{48}, A_{60}, \ldots$

the following dissection of the Iguanodon may prove useful



to verify the claimed series of simple groups.

2.15 More iguanodons via kfarey.sage

For what it is worth, I have computed some more terms in the *iguanodon series*. Here they are

$L_2(7), M_{12}, A_{16}, M_{24}, A_{28}, A_{40}, A_{48}, A_{60}, A_{68}, A_{88}, A_{96}, A_{120}, A_{132}, A_{148}, A_{164}, A_{196}, \ldots$

By construction, the n-th iguanodon group Ig_n (corresponding to the n-th Farey sequence) is a subgroup of the alternating group on its (half)legs. Hence to prove that all remaining iguanodons are alternating groups boils down to proving that they are sufficiently transitive, for example, by showing that there are permutations of certain cycle-types in the group. I'm sure any grouptheorist can crack this problem over lunch, so if you did, please drop a comment.

Clearly, I didn't do the calculations in the archaic way of the previous section which consisted in adding a pair of new legs at the proper place in the spine for every new Farey

number, write down the two generating permutations, giving them to GAP and check simplicity and the isomorphism type.

Instead I used a nice SAGE-package to compute with Farey-symbols written by Chris Kurth and available from his website. As this package is a good tool to experiment hunting for other dinosaur-series of simple groups coming from series of Farey-symbols, Ill include the details for Ig_3 (the example used to outline the construction of the *Iguanodon-series*).

First we need to have the n-th Farey-sequence $F(n)$. There are several short Python programs around to do this, for example this one from the Python-Cookbook. Save it to your sage-directory and name it *fareyseq.py* and load it into sage via *load fareyseq.py*. Then typing *farey(3)* to the sage-prompt spits back

```
sage: farey(3)
  [(1, 3), (1, 2), (2, 3)]
```

That is, 0 and 1 are not included and Farey-numbers are represented by numerator-denominator couples. The iguanodon-series uses the Fareys upto $\frac{1}{2}$, identifies the edges connecting 0 and 1 to ∞ and makes all other intervals odd. That is, the corresponding Farey symbol for F(3) is

$$\infty \overset{}{\underset{1}{\text{———}}} 0 \overset{}{\underset{\bullet}{\text{———}}} \frac{1}{3} \overset{}{\underset{\bullet}{\text{———}}} \frac{1}{2} \overset{}{\underset{\bullet}{\text{———}}} 1 \overset{}{\underset{1}{\text{———}}} \infty$$

(to add to the confusion, I denote odd intervals by a black-bullet whereas in Kulkarni's paper they are white...) Anyway, get Kurth's kfarey-package and save the folder as *kfarey* in your sage-folder. Kurth uses the following notation for Farey-symbols

The *Farey Symbol* is a list $[a, b, p]$ where a is a list of numerators, b a list of denominators, and p the pairing information. If $x[i] = \frac{a[i]}{b[i]}$ then $p[i]$ is the pairing of the side between $x[i-1]$ and $x[i]$. The $p[i]$s can be positive integers, indicating pairing between sides, or -2 or -3, meaning an even or odd pairing respectively.

The above Farey-symbol is therefore represented as

$[[0, 1, 1, 1], [1, 3, 2, 1], [1, -3, -3, -3, 1]]$.

The kfarey-function *LRCosetRep(F)* returns two permutations L and R giving the permutation action of the two generators of the modular group $PSL_2(\mathbb{Z})$

$$L = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad \text{and} \qquad R = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

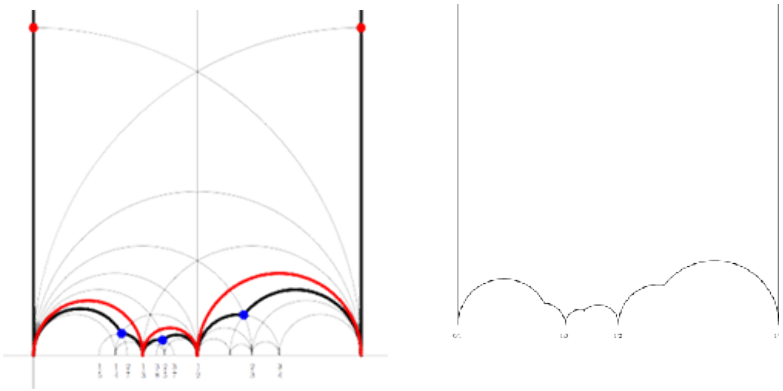
on the half-legs of the inguanodon (the dessin corresponding to the Farey-symbol). Here's the sage transcript

```
sage: load kfarey/farey.sage
sage: load kfarey/conggroups.sage
sage: load kfarey/LR.sage
sage: ig3=[[0,1,1,1],[1,3,2,1],[1,-3,-3,-3,1]]
sage: LRCosetRep(ig3)
   [(1,2,3,9,10,11,6,7,8,4,5)(12), (1,8,4,2,11,6,3,12,10,7,5)(9)]
```

Giving these two generators to GAP one verifies that they indeed generate M_{12}

```
gap> ig3:=Group((1,2,3,9,10,11,6,7,8,4,5)(12),
(1,8,4,2,11,6,3,12,10,7,5)(9));
```

```
   Group([ (1,2,3,9,10,11,6,7,8,4,5), (1,8,4,2,11,6,3,12,10,7,5) ])
gap> IsSimpleGroup(ig3);
    true
gap> IsomorphismTypeInfoFiniteSimpleGroup(ig3);
    rec( series := "Spor", name := "M(12)" )
```



kfarey has plenty of other useful functions. One can even create an .eps file of the fundamental domain specified by the subgroup of the modular group encoded by the Farey symbol using *MakeEpsFile(F)*. For the above example it returns the picture on the right. Not quite as nice as the one on the left, but surely a lot easier to create.

2.16 Farey symbols of sporadic groups

John Conway once wrote :

"There are almost as many different constructions of M_{24} as there have been mathematicians interested in that most remarkable of all finite groups."

We added yet another construction of the Mathieu groups M_{12} and M_{24} starting from (half of) the Farey sequences and the associated cuboid tree diagram obtained by demanding that all edges are odd. In this way the Mathieu groups turned out to be part of a (conjecturally) infinite sequence of simple groups, starting as follows :

$$L_2(7), M_{12}, A_{16}, M_{24}, A_{28}, A_{40}, A_{48}, A_{60}, A_{68}, A_{88}, A_{96}, A_{120}, A_{132}, A_{148}, \ldots$$

It is quite easy to show that none of the other sporadics will appear in this sequence via their known permutation representations. Still, several of the sporadic simple groups are generated by an element of order two and one of order three, so they are determined by a finite dimensional permutation representation of the modular group $PSL_2(\mathbb{Z})$ and hence are hiding in a special polygonal region of the *Dedekind's tessellation*.

Let us try to figure out where the sporadic with the next simplest permutation representation is hiding : the second Janko group J_2, via its 100-dimensional permutation representation. The Atlas tells us that the order two and three generators act as

e:= (1,84)(2,20)(3,48)(4,56)(5,82)(6,67)(7,55)(8,41)(9,35)(10,40)(11,78)(12, 100)

(13,49)(14,37)(15,94)(16,76)(17,19)(18,44)(21,34)(22,85)(23,92)(24, 57)(25,75)

(26,28)(27,64)(29,90)(30,97)(31,38)(32,68)(33,69)(36,53)(39,61) (42,73)(43,91)

(45,86)(46,81)(47,89)(50,93)(51,96)(52,72)(54,74)(58,99) (59,95)(60,63)(62,83)

(65,70)(66,88)(71,87)(77,98)(79,80);

v:= (1,80,22)(2,9,11)(3,53,87)(4,23,78)(5,51,18)(6,37,24)(8,27,60)(10,62,47)

(12,65,31)(13,64,19)(14,61,52)(15,98,25)(16,73,32)(17,39,33)(20,97,58)

(21,96,67)(26,93,99)(28,57,35)(29,71,55)(30,69,45)(34,86,82)(38,59,94)

(40,43,91)(42,68,44)(46,85,89)(48,76,90)(49,92,77)(50,66,88)(54,95,56)

(63,74,72)(70,81,75)(79,100,83);

But as the kfarey.sage package written by Chris Kurth calculates the Farey symbol using the L-R generators, we use GAP to find those

$L = e * v^{-1}$ and $R = e * v^{-2}$, so

L=(1,84,22,46,70,12,79)(2,58,93,88,50,26,35)(3,90,55,7,71,53,36)(4,95,38,65,75,98,92)

(5,86,69,39,14,6,96)(8,41,60,72,61,17, 64)(9,57,37,52,74,56,78)(10,91,40,47,85,80,83)

(11,23,49,19,33,30,20)(13,77,15,59,54,63,27)(16,48,87,29,76,32,42)(18,68, 73,44,51,21,82)

(24,28,99,97,45,34,67)(25,81,89,62,100,31,94)

R=(1,84,80,100,65,81,85)(2,97,69,17,13,92,78)(3,76,73,68,16,90,71)(4,54,72,14,24,35,11)

(5,34,96,18,42,32,44)(6,21,86,30,58, 26,57)(7,29,48,53,36,87,55)(8,41,27,19,39,52,63)

(9,28,93,66,50,99,20)(10,43,40,62,79,22,89)(12,83,47,46,75,15,38)(23,77, 25,70,31,59,56)

(33,45,82,51,67,37,61)(49,64,60,74,95,94,98)

Defining these permutations in sage and using kfarey, this gives us the Farey-symbol of the associated permutation representation

L=SymmetricGroup(Integer(100))(”(1,84,22,46,70,12,79)(2,58,93,88,50,26,35)(3,90,55,7,71,53,36)

(4,95,38,65,75,98,92)(5,86,69,39,14,6,96)(8,41,60,72,61,17, 64)(9,57,37,52,74,56,78)(10,91,40,47,85,80,83)

(11,23,49,19,33,30,20)(13,77,15,59,54,63,27)(16,48,87,29,76,32,42)(18,68, 73,44,51,21,82)

(24,28,99,97,45,34,67)(25,81,89,62,100,31,94)”)

R=SymmetricGroup(Integer(100))(”(1,84,80,100,65,81,85)(2,97,69,17,13,92,78)(3,76,73,68,16,90,71)

(4,54,72,14,24,35,11)(5,34,96,18,42,32,44)(6,21,86,30,58, 26,57)(7,29,48,53,36,87,55)(8,41,27,19,39,52,63)

(9,28,93,66,50,99,20)(10,43,40,62,79,22,89)(12,83,47,46,75,15,38)(23,77, 25,70,31,59,56)

(33,45,82,51,67,37,61)(49,64,60,74,95,94,98)”)

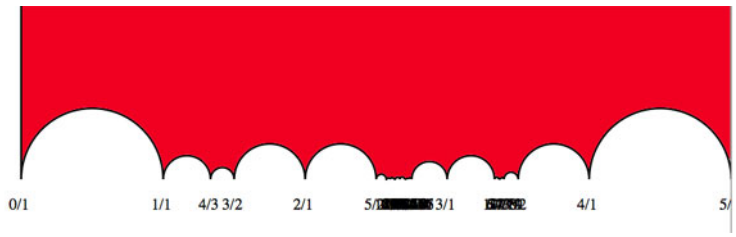
sage: FareySymbol(”Perm”,[L,R])

[[0, 1, 4, 3, 2, 5, 18, 13, 21, 71, 121, 413, 292, 463, 171, 50, 29, 8, 27, 46, 65, 19, 30, 11, 3, 10, 37, 64, 27, 17, 7, 4, 5],

[1, 1, 3, 2, 1, 2, 7, 5, 8, 27, 46, 157, 111, 176, 65, 19, 11, 3, 10, 17, 24, 7, 11, 4, 1, 3, 11, 19, 8, 5, 2, 1, 1],

[-3, 1, 4, 4, 2, 3, 6, -3, 7, 13, 14, 15, -3, -3, 15, 14, 11, 8, 8, 10, 12, 12, 10, 9, 5, 5, 9, 11, 13, 7, 6, 3, 2, 1]]

Here, the first string gives the numerators of the cusps, the second the denominators and the third gives the pairing information (where -2 denotes an even edge and -3 an odd edge. Fortunately, kfarey also allows us to draw the special polygonal region determined by a Farey-symbol. So, here it is (without the pairing data) :



the hiding place of J_2...

It would be nice to have (a) other Farey-symbols associated to the second Janko group, hopefully showing a pattern that one can extend into an infinite family as in the inguanodon series and (b) to determine Farey-symbols of more sporadic groups.

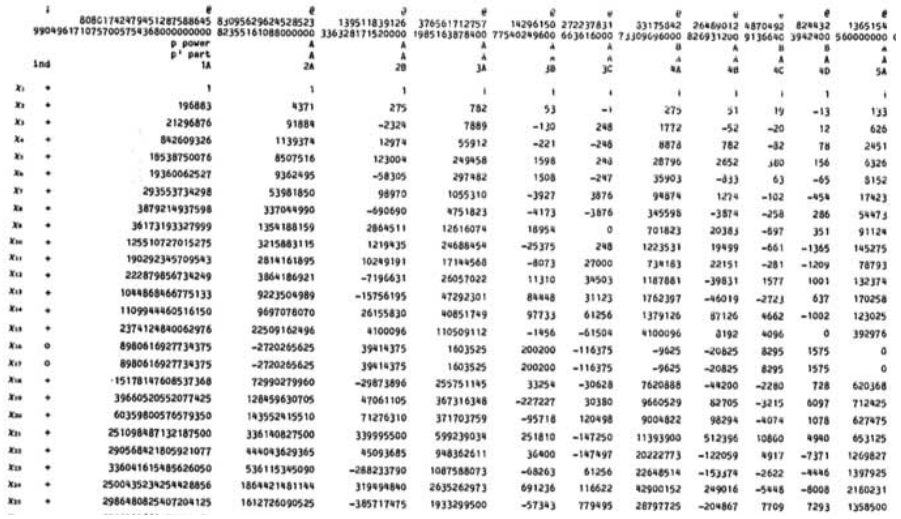
2.17 The McKay-Thompson series

Monstrous moonshine was born (sometime in 1978) the moment John McKay realized that the linear term in the j-function

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864229970q^3 + \dots$$

is surprisingly close to the dimension of the smallest non-trivial irreducible representation of the monster group, which is 196883.

Note that at that time, the Monster hasn't been constructed yet, and, the only traces of its possible existence were kept as semi-secret information in a huge ledger (costing 80 pounds...) kept in the Atlas-office at Cambridge. Included were 8 huge pages describing the character table of the monster, the top left fragment, describing the lower dimensional irreducibles and their characters at small order elements, reproduced below



If you look at the dimensions of the smallest irreducible representations (the first column) : 196883, 21296876, 842609326, ... you will see that the first, second and third of them are extremely close to the linear, quadratic and cubic coefficient of the j-function. In fact, more is true : one can obtain these actual j-coefficients as simple linear combination of the dimensions of the irrducibles :

$$\begin{cases} 196884 & = 1 + 196883 \\ 21493760 & = 1 + 196883 + 21296876 \\ 864229970 & = 2 \times 1 + 2 \times 196883 + 21296876 + 842609326 \end{cases}$$

Often, only the first relation is attributed to McKay, whereas the second and third were supposedly discovered by John Thompson after MKay showed him the first. Marcus du Sautoy tells a somewhat different sory in Finding Moonshine :

"McKay has also gone on to find these extra equations, but is was Thompson who first published them. McKay admits that "I was a bit peeved really, I don't think Thompson quite knew how much I knew."

By the work of Richard Borcherds we now know the (partial according to some) explanation behind these numerical facts : there is a graded representation $V = \oplus_i V_i$ of the Monster-group (actually,

it has a lot of extra structure such as being a vertex algebra) such that the dimension of the i-th factor V_i equals the coefficient f q^i in the j-function. The homogeneous components V_i being finite dimensional representations of the monster, they decompose into the 194 irreducibles X_j. For the first three components we have the decompositions

$$\begin{cases} V_1 &= X_1 \oplus X_2 \\ V_2 &= X_1 \oplus X_2 \oplus X_3 \\ V_3 &= X_1^{\oplus 2} \oplus X_2^{\oplus 2} \oplus X_3 \oplus X_4 \end{cases}$$

Calculating the dimensions on both sides give the above equations. However, being isomorphisms of monster-representations we are not restricted to just computing the dimensions. We might as well compute the character of any monster-element on both sides (observe that the dimension is just the character of the identity element). Characters are the traces of the matrices describing the action of a monster-element on the representation and these numbers fill the different columns of the character-table above.

Hence, the same integral combinations of the character values of any monster-element give another q-series and these are called the McKay-Thompson series. John Conway discovered them to be classical modular functions known as Hauptmoduln.

In most papers and online material on this only the first few coefficients of these series are documented, which may be just too little information to make new discoveries!

Fortunately, David Madore has compiled the first 3200 coefficients of all the 172 monster-series which are available in a huge 8Mb file. And, if you really need to have more coefficients, you can always use and modify his moonshine python program.

In order to reduce bandwidth, here a list containing the first 100 coefficients of the j-function

jfunct=[196884, 21493760, 864299970, 20245856256, 333202640600, 4252023300096, 44656994071935, 401490886656000, 3176440229784420, 22567393309593600, 146211911499519294, 874313719685775360, 4872010111798142520, 25497827389410525184, 126142916465781843075, 593121772421445058560, 2662842413150775245160, 11459912788444786513920, 47438786801234168813250, 189449976248893390028800, 731811377318137519245696, 2740630712513624654929920, 9971041659937182693533820, 35307453186561427099877376, 121883284330422510433351500, 410789960190307909157638144, 1353563541518646878675077500, 4365689224858876634610401280, 13798375834642999925542288376, 42780782244213262567058227200, 130233693825770295128044873221, 389608006170995911894300098560, 1146329398900810637779611090240, 3319627709139267167263679606784, 9468166135702260431646263438600, 26614365825753796268872151875584, 73773169969725069760801792854360, 201768789947228738648580043776000, 544763881751616630123165410477688, 1452689254439362169794355429376000, 3827767751739363485065598331130120, 9970416600217443268739409968824320, 25683334706395406994774011866319670, 65452367731499268312170283695144960, 165078821568186174782496283155142200, 412189630805216773489544457234333696, 1019253515891576791938652011091437835, 2496774105950716692603315123199672320, 6060574415413720999542378222812650932, 14581598453215019997540391326153984000, 34782974253512490652111111930326416268, 82282309236048637946346570669250805760, 193075525467822574167329529658775261720, 449497224123337477155078537760754122752, 1038483010587949794068925153685932435825, 2381407585309922413499951812839633584128, 5421449889876564723000378957979772088000, 12255365475040820661535516233050165760000, 27513411092859486460692553086168714659374, 61354289505303613617069338272284858777600, 135925092428365503809701809166616289474168, 299210983800076883665074958854523331870720, 654553043491650303064385476041569995365270, 1423197635972716062310802114654243653681152, 3076095473477196763039615540128479523917200, 6610091773782871627445909215080641586954240, 14123583372861184908287080245891873213544410, 30010041497911129625894110839466234009518080, 63419842535335416307760114920603619461313664, 133312625293210235328551896736236879235481600, 278775024890624328476718493296348769305198947, 579989466306862709777897124287027028934656000, 1200647685924154079965706763561795395948173320, 2473342981183106509136265613239678864092991488,

507071193089899708057007890628084219651964675 0, 1034690664085042635622631683925982257411594649 6,
2101594581027514325069105890248207991008645952 0, 4249352002468645996896932754140417894123986944 0,
8553998181842497589405376944809879634980864387 8, 1714448430238566323230505079666265543046332416 00,
3421555255551891767319838691235839420119784933 64, 6799868436672140521719540980185825226099449651 20,
1345823847068981684952596216882155845897900827370, 2652886321384703560252232129659440092172381585408,
5208621342520253933693153488396012720448385783600, 1018663549714095683021681120722997561148079760179 2,
1984594685771538724169587808042550486362873888212 5, 3851894383028349736536939133624313888225014579 2000,
7448451892928901781171998983276814207693125941012 0, 1435071724672834538855152223427829911923532076032 00,
2755010426167891537490806178938367969511339297834 96,
5270360580532817641880892200416292011919755057561 60,
1004730453440939042843898965365412981690307145827840,
1908864098321310302488604739098618405938938477379584,
3614432179304462681879676809120464684975130836205250,
6821306832689380776546629825653465084003418476904448,
1283156845093056623704915719101710486121743363428996 0,
2406014344493760499759158609038047341808640169683968 0,
4497219569801180674015081827517775498640947291054964 6,
8379883111070747691275195038475745270380191833907200 0]

This information will come in handy for our *Monstrous Easter Egg Race*.

2.18 Monstrous Easter Egg Race

Here's a sweet Easter egg for you to crack : a mysterious message from none other than the discoverer of Monstrous Moonshine himself...

```
From:  mckayj@Math.Princeton.EDU
Date:  Mon 10 Mar 2008 07:51:16 GMT+01:00
To:    lieven.lebruyn@ua.ac.be

The secret of Monstrous Moonshine and the universe.

Let  j(q) = 1/q + 744 + sum( c[k]*q^k,k>=1) be the Fourier expansion
at oo of the elliptic modular function.

Compute sum(c[k]^2,k=1..24) modulo 70

Background: w_25 of page x of the preface of Conway/Sloane book SPLAG

Also in Chapter 27:
The automorphism group of the 26-dimensional Lorentzian lattice
The Weyl vector w_25 of section 2.

Jm
```

I realize that all of you will feel frustrated by the fact that most university libraries are closed today and possibly tomorrow, hence some help with the background material.

SPLAG of course refers to the cult-book Sphere Packings, Lattices and Groups.

26-dimensional Lorentzian space $\mathbb{R}^{25,1}$ is 26-dimensional real space equipped with the norm-map

$||\vec{v}|| = \sum_{i=1}^{25} v_i^2 - v_{26}^2$

The Weyl vector $\vec{w}_{25}$ is the norm-zero vector in $\mathbb{R}^{25,1}$

$\vec{w}_{25} = (0, 1, 2, 3, 4, \ldots, 22, 23, 24, 70)$ (use the numerical fact that $1^2 + 2^2 + 3^2 + \ldots + 24^2 = 70^2$)

The relevance of this special vector is that it gives a one-line description for one of the most mysterious objects around, the 24-dimensional Leech Lattice L_{24}. In fact

$L_{24} = \vec{w}^{\perp}/\vec{w}$ with $\vec{w}^{\perp} = \vec{x} \in \Pi_{25,1} \ : \ \vec{x}.\vec{w} = 0$

where $\Pi_{25,1}$ is the unique even unimodular lattice in $\mathbb{R}^{25,1}$. These facts amply demonstrate the moonshine nature of the numbers 24 and 70. Apart from this, the list of numbers at the end of the foregoing section may also be of use.

2.19 The secret revealed

Often, one can appreciate the answer to a problem only after having spend some time trying to solve it, and having failed ... pathetically.

When someone with a track-record of coming up with surprising mathematical tidbits like John McKay sends me a *mystery message* claiming to contain "The secret of Monstrous Moonshine and the universe", I'm happy to spend the remains of the day trying to make sense of the apparent nonsense

```
Let j(q) = 1/q + 744 + sum( c[k]*q^k,k>=1) be the Fourier
expansion at oo of the elliptic modular function.
Compute sum(c[k]^2,k=1..24) modulo 70
```

I expected the j-coefficients modulo 70 (or their squares, or their partial sums of squares) to reveal some hidden pattern, like containing the coefficients of Leech vectors or E(8)-roots, or whatever... and spend a day trying things out. But, all I got was *noise*... I left it there for a week or so, rechecked everything and... gave up

```
Subject:   Re: mystery message
From:  lieven.lebruyn@ua.ac.be
Date:  Fri 21 Mar 2008 12:37:47 GMT+01:00
To:    mckayj@Math.Princeton.EDU

i forced myself to recheck the calculations i did once
 after receiving your mail. here are the partial sums
 of squares of j-coefficients modulo 70 for the first
100 of them

[0, 46, 26, 16, 32, 62, 38, 3, 53, 13, 63, 39, 29, 59, 45, 10, 60, 40, 30,
 10, 40, 26, 6, 56, 42, 22, 68, 48, 48, 64, 64, 45, 25, 15, 31, 31, 67,
 47, 7, 21, 51, 31, 31, 61, 21, 1, 17, 12, 2, 16, 46, 60, 20, 10, 54, 49,
 63, 63, 53, 29, 29, 23, 13, 13, 27, 27, 17, 7, 67, 43, 43, 52, 42, 42,
 16, 6, 42, 42, 42, 36, 66, 32, 62, 52, 66, 66, 0, 25, 5, 5, 35, 21, 11,
 11, 57, 57, 61, 41, 41]

term 24 is 42...
i still fail to see the significance of it all.
atb :: lieven.
```

A couple of hours later I received his reply and simply couldn't stop laughing...

```
From:  mckay@encs.concordia.ca
Subject:   Re: mystery message
Date:  Sat 22 Mar 2008 02:33:19 GMT+01:00
To:    lieven.lebruyn@ua.ac.be

I apologize for wasting your time. It is a joke
depending, it seems, on one's cultural background.

See the google entry:
```

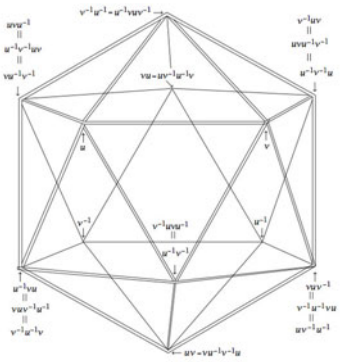
```
Answer to Life, the Universe, and Everything

Best, John McKay
```

Still confused? Well, do it!

2.20 The monster graph and McKay's observation

While the verdict on a neolithic Scottish icosahedron is still open, let us recall Kostant's group-theoretic construction of the icosahedron from its rotation-symmetry group A_5.



The alternating group A_5 has two conjugacy classes of order 5 elements, both consisting of exactly 12 elements. Fix one of these conjugacy classes, say C and construct a graph with vertices the 12 elements of C and an edge between two $u, v \in C$ if and only if the group-product $u.v \in C$ still belongs to the same conjugacy class.

Observe that this relation is symmetric as from $u.v = w \in C$ it follows that $v.u = u^{-1}.u.v.u = u^{-1}.w.u \in C$. The graph obtained is the icosahedron, depicted on the right with vertices written as words in two adjacent elements u and v from C, as indicated.

Kostant writes : "Normally it is not a common practice in group theory to consider whether or not the product of two elements in a conjugacy class is again an element in that conjugacy class. However such a consideration here turns out to be quite productive."

Still, similar constructions have been used in other groups as well, in particular in the study of the largest sporadic group, the monster group $\mathbb{M}$.

There is one important catch. Whereas it is quite trivial to multiply two permutations and verify whether the result is among 12 given ones, for most of us mortals it is impossible to do actual calculations in the monster. So, we'd better have an alternative way to get at the icosahedral graph using only A_5-data that is also available for the monster group, such as its character table.

Let G be any finite group and consider three of its conjugacy classes $C(i), C(j)$ and $C(k)$. For any element $w \in C(k)$ we can compute from the character table of G the number of different products $u.v = w$ such that $u \in C(i)$ and $v \in C(j)$. This number is given by the formula

$$\frac{|G|}{|C_G(g_i)||C_G(g_j)|} \sum_\chi \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_k)}}{\chi(1)}$$

where the sum is taken over all irreducible characters χ and where $g_i \in C(i), g_j \in C(j)$ and $g_k \in C(k)$. Note also that $|C_G(g)|$ is the number of G-elements commuting with g and that this number is the order of G divided by the number of elements in the conjugacy class of g.

The character table of A_5 is given below : the five columns correspond to the different conjugacy classes of elements of order resp. 1,2,3,5 and 5 and the rows are the character functions of the 5 irreducible representations of dimensions 1,3,3,4 and 5.

Let us fix the 4th conjugacy class, that is 5a, as our class C. By the general formula, for a fixed $w \in C$ the number of different products $u.v = w$ with $u, v \in C$ is equal to

$$\frac{60}{25}\left(\frac{1}{1} + \frac{(\frac{1+\sqrt{5}}{2})^3}{3} + \frac{(\frac{1-\sqrt{5}}{2})^3}{3} - \frac{1}{4} + \frac{0}{5}\right) = \frac{60}{25}\left(1 + \frac{4}{3} - \frac{1}{4}\right) = 5$$

```
     1a 2a 3a 5a 5b
  2P 1a 1a 3a 5b 5a
  3P 1a 2a 1a 5b 5a
  5P 1a 2a 3a 1a 1a

X.1     1  1  1  1  1
X.2     3 -1  .  A *A
X.3     3 -1  . *A  A
X.4     4  .  1 -1 -1
X.5     5  1 -1  .  .

A = -E(5)-E(5)^4
  = (1-ER(5))/2 = -b5
```

Because for each $x \in C$ also its inverse $x^{-1} \in C$, this can be rephrased by saying that there are exactly 5 different products $w^{-1}.u \in C$, or equivalently, that the valency of every vertex $w^{-1} \in C$ in the graph is exactly 5.

That is, our graph has 12 vertices, each with exactly 5 neighbors, and with a bit of extra work one can show it to be the icosahedral graph.

For the monster group, the Atlas tells us that it has exactly 194 irreducible representations (and hence also 194 conjugacy classes). Of these conjugacy classes, the involutions (that is the elements of order 2) are of particular importance.

Fig. 2.6: Bernd Fischer

There are exactly 2 conjugacy classes of involutions, usually denoted 2A and 2B. Involutions in class 2A are called "Fischer-involutions", after Bernd Fischer, because their centralizer subgroup is an extension of Fischer's baby Monster sporadic group.

Likewise, involutions in class 2B are usually called "Conway-involutions" because their centralizer subgroup is an extension of the largest Conway sporadic group.

Let us define the *monster graph* to be the graph having as its vertices the Fischer-involutions and with an edge between two of them $u, v \in 2A$ if and only if their product $u.v$ is again a Fischer-involution.

Because the centralizer subgroup is $2.\mathbb{B}$, the number of vertices is equal to

$$97239461142009186000 = 2^4 * 3^7 * 5^3 * 7^4 * 11 * 13^2 * 29 * 41 * 59 * 71.$$

From the general result recalled before we have that the valency in all vertices is equal and to determine it we have to use the character table of the monster and the formula. Fortunately GAP provides the function ClassMultiplicationCoefficient to do this without making errors.

‘

```
gap> table:=CharacterTable("M");
CharacterTable( "M" )
gap> ClassMultiplicationCoefficient(table,2,2,2);
27143910000
```

‘

Fig. 2.7: John McKay

Perhaps noticeable is the fact that the prime decomposition of the valency $27143910000 = 2^4 * 3^4 * 5^4 * 23 * 31 * 47$ is symmetric in the three smallest and three largest prime factors of the baby monster order.

Robert Griess proved that one can recover the monster group $\mathbb{M}$ from the monster graph as its automorphism group!

As in the case of the icosahedral graph, the number of vertices and their common valency does not determine the monster graph uniquely. To gain more insight, we would like to know more about the sizes of minimal circuits in the graph, the number of such minimal circuits going through a fixed vertex, and so on.

Such an investigation quickly leads to a careful analysis which other elements can be obtained from products $u.v$ of two Fischer involutions $u, v \in 2A$. We are in for a major surprise, first observed by John McKay:

Printing out the number of products of two Fischer-involutions giving an element in the i-th conjugacy class of the monster, where i runs over all 194 possible classes, we get the following string of numbers

```
97239461142009186000, 27143910000, 196560, 920808, 0, 3, 1104, 4, 0, 0, 5, 0,
6, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
```

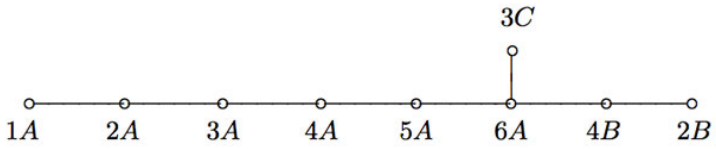
‘

That is, the elements of only 9 conjugacy classes can be written as products of two Fischer-involutions! These classes are :

- 1A = 1 written in 97239461142009186000 different ways (after all involutions have order two)
- 2A, each element of which can be written in exactly 27143910000 different ways (the valency)
- 2B, each element of which can be written in exactly 196560 different ways. Observe that this is the kissing number of the Leech lattice leading to a permutation representation of $2.Co_1$.
- 3A, each element of which can be written in exactly 920808 ways. Note that this number gives a permutation representation of the maximal monster subgroup $3.Fi'_{24}$.
- 3C, each element of which can be written in exactly 3 ways.
- 4A, each element of which can be written in exactly 1104 ways.
- 4B, each element of which can be written in exactly 4 ways.
- 5A, each element of which can be written in exactly 5 ways.
- 6A, each element of which can be written in exactly 6 ways.

Let us forget about the actual numbers for the moment and concentrate on the orders of these 9 conjugacy classes : 1,2,2,3,3,4,4,5,6. These are precisely the components of the fundamental root of the extended Dynkin diagram $\tilde{E}_8$!

This is the content of *John McKay's E(8)-observation* : there should be a precise relation between the nodes of the extended Dynkin diagram and these 9 conjugacy classes in such a way that the order of the class corresponds to the component of the fundamental root. More precisely, one conjectures the following correspondence



This is similar to the classical McKay correspondence between finite subgroups of $SU(2)$ and extended Dynkin diagrams (the binary icosahedral group corresponding to extended E(8)). In that correspondence, the nodes of the Dynkin diagram correspond to irreducible representations of the group and the edges are determined by the decompositions of tensor-products with the fundamental 2-dimensional representation.

Here, however, the nodes have to correspond to conjugacy classes (rather than representations) and we have to look for another procedure to arrive at the required edges! An exciting proposal has been put forward recently by John Duncan in his paper Arithmetic groups and the affine E8 Dynkin diagram.

t will take us a couple of sections to get there, but for now, let's give the gist of it : monstrous moonshine gives a correspondence between conjugacy classes of the monster and certain arithmetic subgroups of $PSL_2(\mathbb{R})$ commensurable with the modular group $\Gamma = PSL_2(\mathbb{Z})$. The edges of the extended Dynkin E(8) diagram are then given by the configuration of the arithmetic groups corresponding to the indicated 9 conjugacy classes!

2.21 Conway's big picture

Fig. 2.8: J.H. Conway, S. Norton

Conway and Norton showed that there are exactly 171 moonshine functions and associated two arithmetic subgroups to them. We want a tool to describe these and here's where Conway's big picture comes in very handy. All moonshine groups are arithmetic groups, that is, they are commensurable with the modular group. Conway's idea is to view several of these groups as point- or set-wise stabilizer subgroups of finite sets of (projective) commensurable 2-dimensional lattices.

Expanding (and partially explaining) the original moonshine observation of McKay and Thompson, John Conway and Simon Norton formulated monstrous moonshine :

To every cyclic subgroup $\langle m \rangle$ of the Monster $\mathbb{M}$ is associated a function

$f_m(\tau) = \frac{1}{q} + a_1 q + a_2 q^2 + \dots$ with $q = e^{2\pi i \tau}$ and all coefficients $a_i \in \mathbb{Z}$ are characters at m of a representation of $\mathbb{M}$. These representations are the homogeneous components of the so called Moonshine module.

Each f_m is a principal modulus for a certain genus zero congruence group commensurable with the modular group $\Gamma = PSL_2(\mathbb{Z})$. These groups are called the moonshine groups.

Conway and Norton showed that there are exactly 171 different functions f_m and associated two arithmetic subgroups $F(m) \subset E(m) \subset PSL_2(\mathbb{R})$ to them (in most cases, but not all, these two groups coincide).

Whereas there is an extensive literature on subgroups of the modular group (see for instance the series of posts starting here), most moonshine groups are *not* contained in the modular group. So, we need a tool to describe them and here's where *Conway's big picture* comes in very handy.

All moonshine groups are arithmetic groups, that is, they are subgroups G of $PSL_2(\mathbb{R})$ which are *commensurable* with the modular group $\Gamma = PSL_2(\mathbb{Z})$ meaning that the intersection $G \cap \Gamma$ is of finite index in both G and in Γ. Conway's idea is to view several of these groups as point- or set-wise stabilizer subgroups of finite sets of (projective) commensurable 2-dimensional lattices.

Start with a fixed two dimensional lattice $L_1 = \mathbb{Z}e_1 + \mathbb{Z}e_2 = \langle e_1, e_2 \rangle$ and we want to name all lattices of the form $L = \langle v_1 = ae_1 + be_2, v_2 = ce_1 + de_2 \rangle$ that are commensurable to L_1. Again this means that the intersection $L \cap L_1$ is of finite index in both lattices. From this it follows immediately that all coefficients a, b, c, d are rational numbers.

It simplifies matters enormously if we do not look at lattices individually but rather at projective equivalence classes, that is $L = \langle v_1, v_2 \rangle \sim L' = \langle v_1', v_2' \rangle$ if there is a rational number $\lambda \in \mathbb{Q}$ such that $\lambda v_1 = v_1', \lambda v_2 = v_2'$. Further, we are of course allowed to choose a different 'basis' for our lattices, that is, $L = \langle v_1, v_2 \rangle = \langle w_1, w_2 \rangle$ whenever $(w_1, w_2) = (v_1, v_2).\gamma$ for some $\gamma \in PSL_2(\mathbb{Z})$. Using both operations we can get any lattice in a specific form. For example,

$$\langle \tfrac{1}{2}e_1 + 3e_2, e_1 - \tfrac{1}{3}e_2 \rangle \overset{(1)}{=} \langle 3e_1 + 18e_2, 6e_1 - 2e_2 \rangle \overset{(2)}{=} \langle 3e_1 + 18e_2, 38e_2 \rangle \overset{(3)}{=} \langle \tfrac{3}{38}e_1 + \tfrac{9}{19}e_2, e_2 \rangle$$

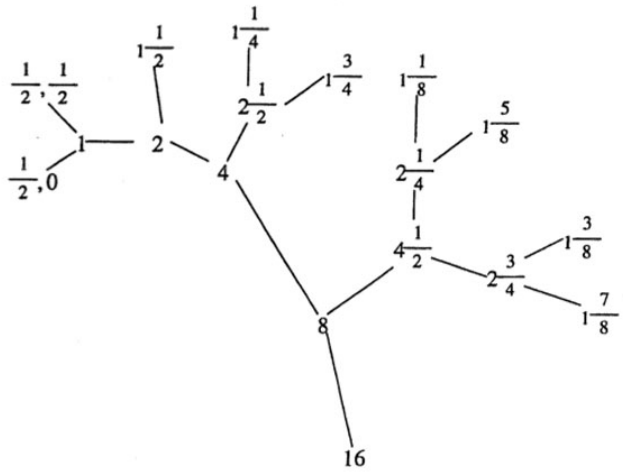
Here, identities (1) and (3) follow from projective equivalence and identity (2) from a base-change. In general, any lattice L commensurable to the standard lattice L_1 can be rewritten uniquely as $L = \langle Me_1 + \frac{g}{h}e_2, e_2 \rangle$ where M a positive rational number and with $0 \leq \frac{g}{h} < 1$.

Another major feature is that one can define a symmetric *hyper-distance* between (equivalence classes of) such lattices. Take $L = \langle Me_1 + \frac{g}{h}e_2, e_2 \rangle$ and $L' = \langle Ne_1 + \frac{i}{j}e_2, e_2 \rangle$ and consider the matrix

$D_{LL'} = \begin{bmatrix} M & \frac{g}{h} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} N & \frac{i}{j} \\ 0 & 1 \end{bmatrix}^{-1}$ and let α be the smallest positive rational number such that all entries of the matrix $\alpha.D_{LL'}$ are integers, then

$\delta(L, L') = det(\alpha.D_{LL'}) \in \mathbb{N}$ defines a symmetric hyperdistance which depends only of the equivalence classes of lattices (**hyper**distance because the log of it behaves like an ordinary distance).

Conway's big picture is the graph obtained by taking as its vertices the equivalence classes of lattices commensurable with L_1 and with edges connecting any two lattices separated by a *prime* number hyperdistance. Here's part of the 2-picture, that is, only depicting the edges of hyperdistance 2.



The 2-picture is an infinite 3-valent tree as there are precisely 3 classes of lattices at hyperdistance 2 from any lattice $L = \langle v_1, v_2 \rangle$ namely (the equivalence classes of) $\langle \frac{1}{2}v_1, v_2 \rangle$, $\langle v_1, \frac{1}{2}v_2 \rangle$ and $\langle \frac{1}{2}(v_1 + v_2), v_2 \rangle$.

Similarly, for any prime hyperdistance p, the p-picture is an infinite p+1-valent tree and the *big picture* is the product over all these prime trees. That is, two lattices at square-free hyperdistance $N = p_1 p_2 \dots p_k$ are two corners of a k-cell in the big picture! (Astute readers of this blog (if such people exist...) may observe that Conway's big picture did already appear here prominently, though in disguise. More on this another time).

The big picture presents a simple way to look at arithmetic groups and makes many facts about them visually immediate. For example, the point-stabilizer subgroup of L_1 clearly is the modular group $PSL_2(\mathbb{Z})$. The point-stabilizer of any other lattice is a certain conjugate of the modular group inside $PSL_2(\mathbb{R})$. For example, the stabilizer subgroup of the lattice $L_N = \langle Ne_1, e_2 \rangle$ (at hyperdistance N from L_1) is the subgroup

$$\begin{bmatrix} a & \frac{b}{N} \\ Nc & d \end{bmatrix} \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in PSL_2(\mathbb{Z})$$

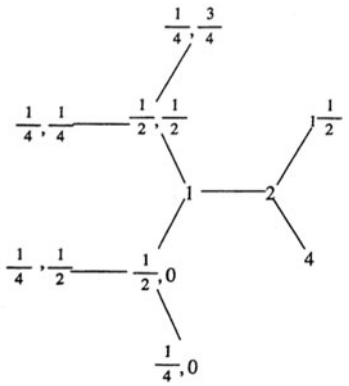


Fig. 2.9: the 4-ball

Now the intersection of these two groups is the modular subgroup $\Gamma_0(N)$ (consisting of those modular group element whose lower left-hand entry is divisible by N). That is, the proper way to look at this arithmetic group is as the joint stabilizer of the two lattices L_1, L_N. The picture makes it trivial to compute the index of this subgroup.

Consider the ball $B(L_1, N)$ with center L_1 and hyper-radius N (on the left, the ball with hyper-radius 4). Then, it is easy to show that the modular group acts transitively on the boundary lattices (including the lattice L_N), whence the index $[\Gamma : \Gamma_0(N)]$ is just the number of these boundary lattices. For N=4 the picture shows that there are exactly 6 of them. In general, it follows from our knowledge of all the p-trees the number of all lattices at hyperdistance N from L_1 is equal to $N \prod_{p|N}(1 + \frac{1}{p})$, in accordance with the well-known index formula for these modular subgroups!

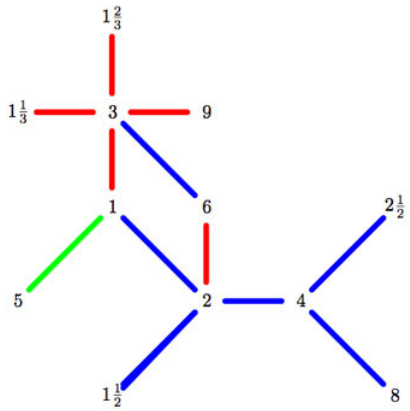
But, there are many other applications of the big picture giving a simple interpretation for the Hecke operators, an elegant proof of the Atkin-Lehner theorem on the normalizer of $\Gamma_0(N)$ (the whimsical source of appearances of the number 24) and of Helling's theorem characterizing maximal arithmetical groups inside $PSL_2(\mathbb{C})$ as conjugates of the normalizers of $\Gamma_0(N)$ for square-free N. J.H. Conway's paper "Understanding groups like $\Gamma_0(N)$" containing all this material is a must-read! Unfortunately, I do not know of an online version.

2.22 Looking for the moonshine picture

We have seen that *Conway's big picture* helps us to determine all arithmetic subgroups of $PSL_2(\mathbb{R})$ commensurable with the modular group $PSL_2(\mathbb{Z})$, including all groups of monstrous moonshine.

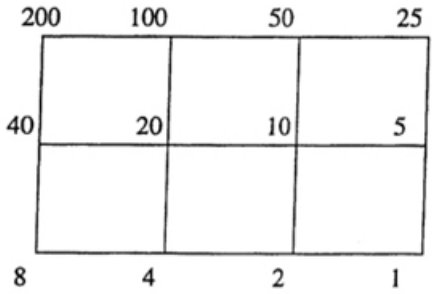
As there are exactly 171 such moonshine groups, they are determined by a finite subgraph of Conway's picture and we call the minimal such subgraph the **moonshine picture**. Clearly, we would like to determine its structure.

Below is a depiction of a very small part of it. It is the minimal subgraph of Conway's picture needed to describe the 9 moonshine groups appearing in Duncan's realization of McKay's E(8)-observation. Here, only three primes are relevant : 2 (blue lines), 3 (reds) and 5 (green). All lattices are number-like (recall that $M\frac{g}{h}$ stands for the lattice $\langle Me_1 + \frac{g}{h}e_2, e_2 \rangle$).



We observe that a large part of this mini-moonshine picture consists of the three *p-tree* subgraphs (the blue, red and green tree starting at the 1-lattice $1 = \langle e_1, e_2 \rangle$. Whereas Conway's big picture is the product over all p-trees with p running over all prime numbers, we observe that the mini-moonshine picture is a very small subgraph of the product of these three subtrees. In fact, there is just one 2-cell (the square 1,2,6,3).

Hence, it seems like a good idea to start our investigation of the full moonshine picture with the determination of the p-subtrees contained in it, and subsequently, worry about higher dimensional cells constructed from them. Surely it will be no major surprise that the prime numbers p that appear in the moonshine picture are exactly the prime divisors of the order of the monster group, that is p=2,3,5,7,11,13,17,19,23,29,31,41,47,59 or 71. Before we can try to determine these 15 p-trees, we need to know more about the 171 moonshine groups.



Recall that the proper way to view the modular subgroup $\Gamma_0(N)$ is as the subgroup fixing the two lattices L_1 and L_N, whence we will write $\Gamma_0(N) = \Gamma_0(N|1)$, and, by extension we will denote with $\Gamma_0(X|Y)$ the subgroup fixing the two lattices L_X and L_Y.

As $\Gamma_0(N)$ fixes L_1 and L_N it also fixes all lattices in the *(N—1)-thread*, that is all lattices occurring in a shortest path from L_1 to L_N (above a picture of the (200—1)-thread).

If $N = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, then the (N—1)-thread has 2^k involutions as symmetries, called the *Atkin-Lehner involutions*. For every exact divisor $e||N$ (that is, $e|N$ and $gcd(e, \frac{N}{e}) = 1$ we have an involution W_e which acts by sending each point in the thread-cell corresponding to the prime divisors of e to its antipodal cell-point and acts as the identity on the other prime-axes. For example, in the (200—1)-thread on the left, W_8 is the left-right reflexion, W_{25} the top-bottom reflexion and W_{200} the antipodal reflexion. The set of all exact divisors of N becomes the group $(\mathbb{Z}/2\mathbb{Z})^k$ under the operation $e * f = \frac{e \times f}{gcd(e,f)^2}$.

Most of the moonshine groups are of the form $\Gamma_0(n|h)+e,f,g,...$ for some $N=h.n$ such that $h|24$ and $h^2|N$. The group $\Gamma_0(n|h)$ is then conjugate to the modular subgroup $\Gamma_0(\frac{n}{h})$ by the element $\begin{bmatrix} h & 0 \\ 0 & 1 \end{bmatrix}$. With $\Gamma_0(n|h)+e,f,g,...$ we mean that the group $\Gamma_0(n|h)$ is extended with the involutions $W_e, W_f, W_g, ...$ If we simply add all Atkin-Lehner involutions we write $\Gamma_0(n|h)+$ for the resulting group.

Finally, whenever $h \neq 1$ there is a subgroup $\Gamma_0(n||h)+e,f,g,...$ which is the kernel of a character λ being trivial on $\Gamma_0(N)$ and on all involutions W_e for which every prime dividing e also divides $\frac{n}{h}$, evaluating to $e^{\frac{2\pi i}{h}}$ on all cosets containing $\begin{bmatrix} 1 & \frac{1}{h} \\ 0 & 1 \end{bmatrix}$ and to $e^{\pm\frac{2\pi i}{h}}$ for cosets containing $\begin{bmatrix} 1 & 0 \\ n & 0 \end{bmatrix}$ (with a + sign if $\begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}$ is present and a - sign otherwise). Btw. it is not evident at all that this is a character, but hard work shows it is!

Clearly there are heavy restrictions on the numbers that actually occur in moonshine. In the paper On the discrete groups of moonshine, John Conway, John McKay and Abdellah Sebbar characterized the 171 arithmetic subgroups of $PSL_2(\mathbb{R})$ occuring in monstrous moonshine as those of the form $G=\Gamma_0(n||h)+e,f,g,...$ which are

(a) of genus zero, meaning that the quotient of the upper-half plane by the action of $G \subset PSL_2(\mathbb{R})$ by Moebius-transformations gives a Riemann surface of genus zero,

(b) the quotient group $G/\Gamma_0(nh)$ is a group of exponent 2 (generated by some Atkin-Lehner involutions), and

(c) every cusp can be mapped to ∞ by an element of $PSL_2(\mathbb{R})$ which conjugates the group to one containing $\Gamma_0(nh)$.

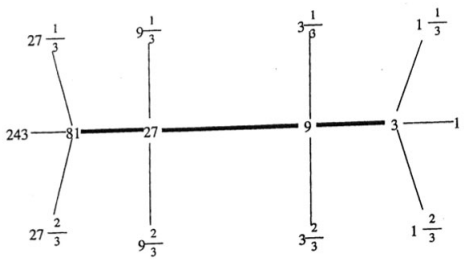
Now, if $\Gamma_0(n||h)+e,f,g,...$ is of genus zero, so is the larger group $\Gamma_0(n|h)+e,f,g,...$, which in turn, is conjugated to the group $\Gamma_0(\frac{n}{h})+e,f,g,....$ Therefore, we need a list of all groups of the form $\Gamma_0(\frac{n}{h})+e,f,g,...$ which are of genus zero. There are exactly 123 of them, listed on the right.

1+	17+	36 + 36
2−	18−	36+
2+	18 + 2	38+
3−	18 + 9	39 + 39
3+	18 + 18	39+
4−	18+	41+
4+	19+	42 + 3, 14, 42
5−	20 + 4	42 + 6, 14, 21
5+	20 + 20	42+
6−	20+	44+
6 + 2	21 + 3	45+
6 + 3	21 + 21	46 + 23
6 + 6	21+	46+
6+	22 + 11	47+
7−	22+	49+
7+	23+	50 + 50
8−	24 + 8	50+
8+	24 + 24	51+
9−	24+	54+
9+	25−	55+
10−	25+	56+
10 + 2	26 + 26	59+
10 + 5	26+	60 + 4, 15, 60
10 + 10	27+	60 + 12, 15, 20
10+	28 + 7	60+
11+	28+	62+
12−	29+	66 + 6, 11, 66
12 + 3	30 + 15	66+
12 + 4	30 + 2, 15, 30	69+
12 + 12	30 + 3, 5, 15	70 + 10, 14, 35
12+	30 + 5, 6, 30	70+
13−	30 + 6, 10, 15	71+
13+	30+	78 + 6, 26, 39
14 + 7	31+	78+
14 + 14	32+	87+
14+	33 + 11	92+
15 + 5	33+	94+
15 + 15	34+	95+
15+	35 + 35	105+
16−	35+	110+
16+	36 + 4	119+

How does this help to determine the structure of the p-subtree of the moonshine picture for the fifteen monster-primes p? Look for the largest p-power p^k such that $p^k+e,f,g...$ appears in the list. That is for p=2,3,5,7,11,13,17,19,23,29,31,41,47,59,71 these powers are resp. 5,3,2,2,1,1,1,1,1,1,1,1,1,1,1. Next, look for the largest p-power p^l dividing 24 (that is, 3 for p=2, 1 for p=3 and 0 for all other primes). Then, these relevant moonshine groups contain the modular subgroup $\Gamma_0(p^{k+2l})$ and are contained in its normalizer in $PSL_2(\mathbb{R})$ which by the Atkin-Lehner theorem is precisely the group $\Gamma_0(p^{k+l}|p^l)+$.

Right, now the lattices fixed by $\Gamma_0(p^{k+2l})$ (and permuted by its normalizer), that is the lattices in our p-subtree, are those that form the $(p^{k+2l}|1)$-*snake* in Conway-speak. That is, the lattices whose hyper-distance to the $(p^{k+l}|p^l)$-thread divides 24. So for all primes larger than 2 or 3, the p-tree is just the $(p^l|1)$-thread.

For p=3 the 3-tree is the (243—1)-snake having the (81—3)-thread as its spine. It contains the following lattices, all of which are number-like.



Depicting the 2-tree, which is the (2048—1)-snake may take a bit longer... Perhaps someone should spend some time figuring out which cells of the product of these fifteen trees make up the *moonshine picture*!

2.23 $E(8)$ from moonshine groups

Are the valencies of the 171 moonshine groups compatible, that is, can one construct a (disconnected) graph on the 171 vertices such that in every vertex (determined by a moonshine group G) the vertex-valency coincides with the valency of the corresponding group? Duncan describes a subset of 9 moonshine groups for which the valencies are compatible. These 9 groups are characterized as those moonshine groups G having width 1 at the cusp and such that their intersection with the modular group is big.

Fig. 2.10: John Duncan

Time to wrap up this series on John Duncan's paper Arithmetic groups and the affine E8 Dynkin diagram in which he gives a realization of the extended E(8)-Dynkin diagram (together with its isotropic root vector) from the moonshine groups, compatible with McKay's E(8)-observation.

In the previous section, we described all 171 moonshine groups using *Conway's big picture*. This description will allow us to associate two numbers to a moonshine group $G \subset PSL_2(\mathbb{R})$. Recall that for any such group we have a positive integer N such that

$$\Gamma_0(N) \subset G \subset \Gamma_0(h, \tfrac{N}{h})+$$

where h is the largest divisor of 24 such that $h^2|N$. Let us call $n_G = \frac{N}{h}$ the *dimension* of G (Duncan calls this number the 'normalized level') as it will give us the dimension component at the vertex determined by G.

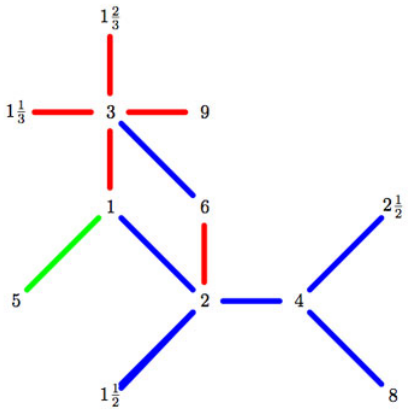
We have also seen last time that any moonshine group is of the form $G = \Gamma_0(n_G||h) + e, f, g$, that is, $G/\Gamma_0(n_G||h)$ is an elementary abelian group $(\mathbb{Z}/2\mathbb{Z})^m$ generated by Atkin-Lehner involutions. Let's call $v_G = m + 1$ the *valency* of the group G as it will give s the valency of the vertex determined by G.

Duncan describes a subset of 9 moonshine groups for which the valencies *are* compatible. These 9 groups are characterized as those moonshine groups G having width 1 at the cusp and such that their intersection with the modular group $\Gamma = PSL_2(\mathbb{Z})$ is big, more precisely the index $[\Gamma : \Gamma \cap G] \leq 12$ and $[\Gamma : \Gamma \cap G]/[G : \Gamma \cap G] \leq 3$.

They can be described using the mini-moonshine picture below. They are :

The modular group itself $1 = \Gamma$, being the stabilizer of the lattice 1. This group has clearly dimension and valency equal to one.

The modular subgroup $2 = \Gamma_0(2)$ being the point-wise stabilizer of the lattices 1 and 2 (so it has valency one and dimension two, and, its normalizer $2+ = \Gamma_0(2)+$ which is the set-wise stabilizer of the lattices 1 and 2 and the one Atkin-Lehner involution interchanges both. So, this group has valency two (as we added one involution) as well as dimension two.



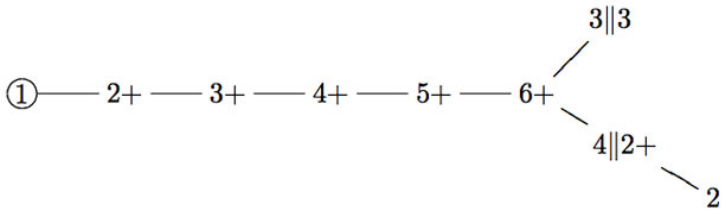
Likewise, the groups $3+ = \Gamma_0(3)+$ and $5+ = \Gamma_0(5)+$ are the stabilzer subgroups of the red 1-cell (1,3) resp. the green 1-cell (1,5) and hence have valency two (as we add one involution) and dimensions 3 resp. 5.

The group $4+ = \Gamma_0(4)+$ stabilizes the (1—4)-thread and as we add one involution must have valency 2 and dimension 4.

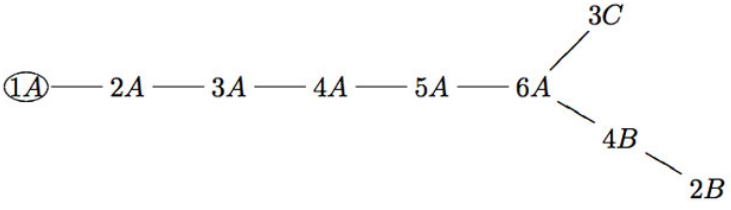
On the other hand, the group $6+ = \Gamma_0(6)+$ stabilizes the unique 2-cell in the picture (having lattices 1,2,3,6) so this time we will add three involutions (horizontal and vertical switches and their product the antipodal involution). Hence, for this group the valency is three and its dimension is equal to six.

Remain the two groups connected to the *mini-snakes* in the picture. The red mini-snake (top left hand) is the ball with center 3 and *hyper-distance* 3 and determines the group $3||3 = \Gamma_0(3||3)$ which has valency one (we add no involutions) and dimension 3. The blue mini-snake (the extended D(5)-Dynkin in the lower right corner) determines the group $4||2+ = \Gamma(4||2)+$ which has valency two and dimension 4.

The valencies of these 9 moonshine groups are compatible and they can be arranged in the extended E(8) diagram depicted below



Moreover, the dimensions of the groups give the exact dimension-components of the isotropic root of the extended E(8)-diagram. Further, the dimension of the group is equal to the order of the elements making up the conjugacy class of the monster to which exactly the given groups correspond via monstrous moonshine and hence compatible with John McKay's original E(8)-observation!



Once again, I would love to hear when someone has more information on the cell-decomposition of the *moonshine picture* or if someone can extend the moonshine E(8)-graph, possibly to include all 171 moonshine groups.

2.24 Hexagonal moonshine

Hexagons keep on popping up in the representation theory of the modular group and its close associates.

Let's find representations of the extended modular group $\tilde{\Gamma} = PGL_2(\mathbb{Z})$, which is obtained by adding to the modular group

$$\Gamma = \langle U = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, V = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \rangle \text{ the matrix } R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

In terms of generators and relations, one easily verfifies that

$$\tilde{\Gamma} = \langle\, U, V, R \mid U^2 = R^2 = V^3 = (RU)^2 = (RV)^2 = 1 \,\rangle$$

and therefore $\tilde{\Gamma}$ is the *amalgamated free product* of the dihedral groups D_2 and D_3 over their common subgroup $C_2 = \langle\, R \,\rangle$, that is

$$\tilde{\Gamma} = \langle U, R | U^2 = R^2 = (RU)^2 = 1 \rangle *_{\langle R | R^2 = 1 \rangle} \langle V, R | V^3 = R^2 = (RV)^2 = 1 \rangle = D_2 *_{C_2} D_3$$

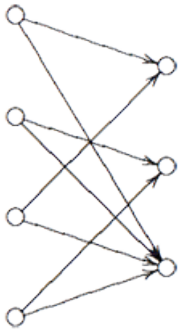
From this description it is easy to find all n-dimensional $\tilde{\Gamma}$-representations V and relate them to quiver-representations. $D_2 = C_2 \times C_2$ and hence has 4 1-dimensonal simples S_1, S_2, S_3, S_4. Restricting $V \downarrow_{D_2}$ to the subgroup D_2 it decomposes as

$$V \downarrow_{D_2} \simeq S_1^{\oplus a_1} \oplus S_2^{\oplus a_2} \oplus S_3^{\oplus a_3} \oplus S_4^{\oplus a_4} \text{ with } a_1 + a_2 + a_3 + a_4 = n$$

Similarly, because $D_3 = S_3$ has two one-dimensional representations T, S (the trivial and the sign representation) and one simple 2-dimensional representation W, restricting V to this subgroup gives a decomposition

$$V \downarrow_{D_3} \simeq T^{b_1} \oplus S^{\oplus b_2} \oplus W^{\oplus b_3}, \text{ this time with } b_1 + b_2 + 2b_3 = n$$

Restricting both decompositions further down to the common subgroup C_2 one obtains a C_2-isomorphism $\phi : V \downarrow_{D_2} \longrightarrow V \downarrow_{D_3}$ which implies also that the above numbers must be chosen such that $a_1 + a_3 = b_1 + b_3$ and $a_2 + a_4 = b_2 + b_3$. We can summarize all this info about V in a representation of the quiver



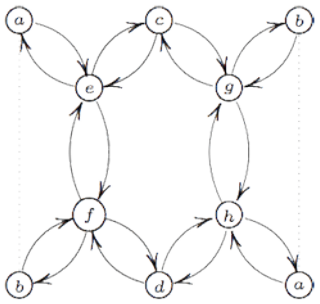
Here, the vertex spaces on the left are the iso-typical factors of $V \downarrow_{D_2}$ and those on the right those of $V \downarrow_{D_3}$ and the arrows give the block-components of the C_2-isomorphism ϕ.

The nice things is that one can also reverse this process to get all $\tilde{\Gamma}$-representations from θ-semistable representations of this quiver (having the additional condition that the square matrix made of the arrows is invertible) and isomorphisms of group-representation correspond to those of quiver-representations!

This proves that for all n the varieties of n-dimensional representations $\mathbf{rep}_n\, \tilde{\Gamma}$ are smooth (but have several components corresponding to the different dimension vectors $(a_1, a_2, a_3, a_4; b_1, b_2, b_3)$ such that $\sum a_i = n = b_1 + b_2 + 2b_3$.

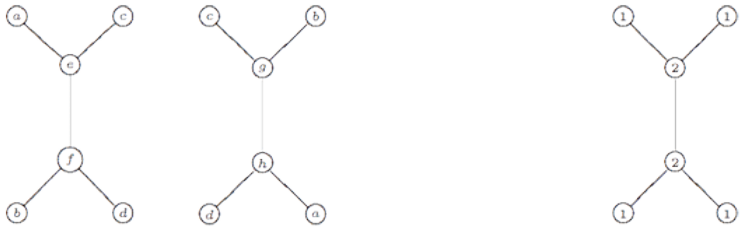
The basic principle of noncommutative geometry is that a lot of the representation theory follows from the 'one quiver' determined by the simples of smallest dimensions. In the case of the extended modular group $\tilde{\Gamma}$ it follows that there are exactly 4 one-dimensional simples and exactly 4 2-dimensional simples, corresponding to the dimension vectors

$$\begin{cases} a=(0,0,0,1;0,1,0) \\ b=(0,1,0,0;0,1,0) \\ c=(1,0,0,0;1,0,0) \\ d=(0,0,1,0;1,0,0) \end{cases} \quad \text{resp.} \quad \begin{cases} e=(0,1,1,0;0,0,1) \\ f=(1,0,0,1;0,0,1) \\ g=(0,0,1,1;0,0,1) \\ h=(1,1,0,0;0,0,1) \end{cases}$$



If one calculates the 'one quiver' of these 8 simples one obtains the double quiver of the graph on the left. Note that a and b appear twice, so one should glue the left and right hand sides together as a Moebius-strip. That is, the clan determining the representation theory of the extended modular group is a Moebius strip made of two hexagons!

However, one should not focuss too much on the hexagons (that is, the extended Dynkin diagram $\tilde{A}_5$) here. The two 'backbones' (e–f and g–h) have their vertices corresponding to 2-dimensional simples whereas the top and bottom vertices correspond to one-dimensional simples. Hence, the correct way to look at this clan is as two copies of the double quiver of the extended Dynkin diagram $\tilde{D}_5$ glued over their leaf vertices to form a Moebius strip. Remark that the components of the sotropic root of $\tilde{D}_5$ give the dimensions of the corresponding $\tilde{\Gamma}$ simples.



The remarkable ubiquity of (extended) Dynkins never ceases to amaze!